VERITAS™

VERITAS NetBackup™ 5.1 NetWare® Media Server Option

System Administrator's Guide

for UNIX and Windows

N123498

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

VERITAS Legal Notice

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000 Fax 650–527–2908
www.veritas.com

Third-Party Copyrights

ST. BERNARD Software, Inc.

Contents

Preface

This comprehensive manual provides detailed information and procedures for installing, configuring, and using the VERITAS NetBackup NetWare Media Server Option. Topics covered in this manual require the reader to have a working knowledge of the VERITAS NetBackup and the NetWare operating system. This manual is intended for the system administrator and other users.

What Is In This Manual?

- Chapter 1 provides an overview of the NetBackup NetWare Media Server Option and its features.
- Chapter 2 provides installation procedures for the NetBackup NetWare Media Server Option and the Open File Backup Option and Intelligent Disaster Recovery options that come with it. This section also describes the installation requirements.
- Chapter 3 provides the steps for granting NetBackup access to the NetWare media server, and for setting up NetBackup to use the NetWare Media Server Option.
- Chapter 4 explains how to create manual backups of and restore data to the NetWare server using NetBackup and the NetWare Media Server Option and how to use the Open File Backup Option included with the NetWare Media Server Option.
- Chapter 5 describes how to use the Intelligent Disaster Recovery (IDR) Option, an option designed to help you quickly and efficiently recover your Novell NetWare servers after a catastrophic disaster.

Getting Help

VERITAS offers you a variety of support options.

Accessing the VERITAS Technical Support Web Site

The VERITAS Support Web site allows you to:

- obtain updated information about VERITAS NetBackup, including system requirements, supported platforms, and supported peripherals
- contact the VERITAS Technical Support staff and post questions to them
- get the latest patches, upgrades, and utilities
- view the VERITAS NetBackup Frequently Asked Questions (FAQ) page
- search the knowledge base for answers to technical support questions
- receive automatic notice of product updates
- find out about VERITAS NetBackup training
- read current white papers related to VERITAS NetBackup

The address for the VERITAS Technical Support Web site follows:

- http://support.veritas.com

Subscribing to VERITAS Email Notification Service

Subscribe to the VERITAS Email notification service to be informed of software alerts, newly published documentation, Beta programs, and other services.

Go to http://support.veritas.com. Select a product and click "E-mail Notifications" on the right side of the page. Your customer profile ensures you receive the latest VERITAS technical information pertaining to your specific interests.

Accessing VERITAS Telephone Support

Telephone support for VERITAS NetBackup is only available with a valid support contract. To contact VERITAS for technical support, dial the appropriate phone number listed on the Technical Support Guide included in the product box and have your product license information ready for quick navigation to the proper support group.

▼ **To locate the telephone support directory on the VERITAS web site**

1. Open http://support.veritas.com in your web browser.
2. Click the **Phone Support** icon. A page that contains VERITAS support numbers from around the world appears.

Accessing VERITAS E-mail Support

▼ **To contact support using E-mail on the VERITAS web site**

1. Open http://support.veritas.com in your web browser.
2. Click the **E-mail Support** icon. A brief electronic form will appear and prompt you to:
   - Select a language of your preference
   - Select a product and a platform
   - Associate your message to an existing technical support case
   - Provide additional contact and product information, and your message
3. Click **Send Message**.

Contacting VERITAS Licensing

For license information call 1-800-634-4747 option 3, fax 1-650-527-0952, or e-mail amercustomercare@veritas.com.

VERITAS NetBackup Manuals

The CD-ROM for each NetBackup product has a copy of the related manuals in Adobe Portable Document Format (PDF). The PDF files are either in the root directory or the `Docs` directory on the CD-ROM.

To view the PDF copies of the manuals, you need an Adobe Acrobat reader, which you can download from the Adobe web site at http://`www.adobe.com`. VERITAS assumes no responsibility for the correct installation or use of the reader.

Release Notes

- *VERITAS NetBackup Release Notes for UNIX and Windows*

  NetBackup_Release_Notes.pdf

  Provides important information about NetBackup on UNIX- and Windows-based servers, such as the platforms and operating systems that are supported and operating notes that may not be in the NetBackup manuals or the online help.

Installation Guides

- *VERITAS NetBackup Installation Guide for UNIX*

  NetBackup_Install_UNIX.pdf

  Explains how to install NetBackup software on UNIX-based platforms.

- *VERITAS NetBackup Installation Guide for Windows*

  NetBackup_Install_Windows.pdf

  Explains how to install NetBackup software on Windows-based platforms.

- *VERITAS Security Services Installation Guide*

  VXSS_InstallGuide.pdf on VERITAS Security Services CD-ROM

  Explains how to install and configure the VERITAS Security Services.

System Administrator's Guides - Basic Product

- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume I*

  NetBackup_AdminGuideI_UNIXServer.pdf

  Explains how to configure and manage NetBackup on a UNIX server, including managing storage units, backup policies, catalogs, and host properties.

- *VERITAS NetBackup System Administrator's Guide for UNIX, Volume II*

  NetBackup_AdminGuideII_UNIXServer.pdf

  Explains additional NetBackup features such as access control and enhanced authorization and authentication, and role-based security. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

- *VERITAS NetBackup System Administrator's Guide for Windows, Volume I*

  NetBackup_AdminGuideI_WinServer.pdf

  Explains how to configure and manage NetBackup on a Windows server, including managing storage units, backup policies, catalogs, and host properties.

- *VERITAS NetBackup System Administrator's Guide for Windows, Volume II*

  NetBackup_AdminGuideII_WinServer.pdf

  Explains additional NetBackup features such as access control and enhanced authorization and authentication, and role-based security. The guide also discusses using NetBackup with AFS and Intelligent Disaster Recovery (IDR).

- *VERITAS NetBackup Media Manager System Administrator's Guide for UNIX*

  MediaMgr_AdminGuide_Unix.pdf

  Explains how to configure and manage the storage devices and media on UNIX servers running NetBackup. Media Manager is part of NetBackup.

- *VERITAS NetBackup Media Manager System Administrator's Guide for Windows*

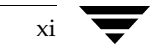
  MediaMgr_AdminGuide_Win.pdf

  Explains how to configure and manage the storage devices and media on Windows servers running NetBackup. Media Manager is part of NetBackup.

- *VERITAS Security Services Administrator's Guide*

  VXSS_AdminGuide.pdf on VERITAS Security Services CD-ROM

  Explains how to configure and manage core security mechanisms, including authentication, protected communications, and authorization.



System Administrator's Guides - Agents and Options

- *VERITAS NetBackup for NDMP System Administrator's Guide*

  NetBackup_AdminGuide_NDMP.pdf

  Explains how to install, configure, and use NetBackup for NDMP to control backups on an NDMP host.

  For more information about NDMP, see the following web site:

  ```
  http://www.ndmp.org
  ```

- *VERITAS NetBackup Advanced Reporter System Administrator's Guide for UNIX and Windows*

  NetBackup_AdminGuide_AdvancedReporter.pdf

  Explains how to install, configure, and use NetBackupAdvanced Reporter to monitor and report on NetBackup activities.

User's Guides

- *VERITAS NetBackup Backup, Archive, and Restore Getting Started Guide*

  NetBackup_BAR_GS_Guide.pdf

  Explains how to use NetBackup on both the UNIX client and the Windows client to perform backups, archives, and restores.

- *VERITAS NetBackup Administrator's Guide for Novell NetWare Client*

  NetBackup_AdminGuide_NetWare_Client.pdf

  Explains how to install and use the NetBackup's NetWare Client software. With the NetWare Client, full and incremental backups can be scheduled to occur automatically and unattended under the control of the NetBackup master server. The NetWare Client also provides two methods for performing user-directed backups and restores: Target, which uses a character-based, menu-driven interface running on the NetWare server, and NonTarget, which uses the NetBackup for NetWare NonTarget Browser that is installed and run from a Windows computer.

Device Configuration Guide - Media Manager

- *VERITAS NetBackup Media Manager Device Configuration Guide for UNIX and Windows*

  MediaMgr_DeviceConfig_Guide.pdf

  Explains how to add device drivers and perform other system-level configurations for storage devices and media servers (or SAN media servers) that are supported by NetBackup Media Manager.

Troubleshooting Guides

- *VERITAS NetBackup Troubleshooting Guide for UNIX and Windows*

  NetBackup_Troubleshoot_Guide.pdf

  Provides troubleshooting information for UNIX- and Windows-based NetBackup products, including Media Manager.

NetBackup Commands

- *VERITAS NetBackup Commands for UNIX*

  NetBackup_Commands_UNIX.pdf

  Describes NetBackup and Media Manager commands and processes that can be run from a UNIX command line.

- *VERITAS NetBackup Commands for Windows*

  NetBackup_Commands_Windows.pdf

  Describes NetBackup and Media Manager commands and processes that can be run from a Windows command prompt.

Online Documentation

On Windows Servers

The released software contains on-line PDF and ASCII versions of these release notes and a readme file for the client. If you choose to install the documentation during setup, NetBackup installs these documents in the following locations on your disk:

- *install_path*\Help\

  Adobe Acrobat Portable Document Format (PDF) copies of all related documents, including these release notes.

- The readme files on *install_path*\NetBackup\ are:
  - Readme.txt (The Readme.txt file (ASCII format) may be slightly more up-to-date than the printed and pdf copies of the release notes.)
  - Readme_Client.txt
  - Readme_Server.txt
  - Readme_SMS.txt
  - Readme_Win2000.txt

On UNIX

During NetBackup installation, a text copy of the *NetBackup Media Manager Device Configuration Guide* is installed in

/usr/openv/volmgr/MediaMgr_DeviceConfig_Guide.txt

You can copy example code from the device configuration guide if you need to reconfigure the kernel to provide specific tape or optical peripheral support.

The product CD-ROM also contains PDF copies of these release notes and other documents.

Note You will need Adobe Acrobat Reader to view the PDF documents. The latest version of Acrobat Reader is available on the Adobe web site: http://www.adobe.com.
VERITAS assumes no responsibility for the correct installation or use of the reader.

Glossary

If you encounter unfamiliar terminology, consult the NetBackup online glossary. The glossary contains terms and definitions for NetBackup and all additional NetBackup options and agents.

The NetBackup online glossary is included in the NetBackup help file.

▼ **To access the NetBackup online glossary**

1. In the NetBackup Administration Console, click **Help** > **Help Topics**.
2. Click the **Contents** tab.
3. Click **Glossary of NetBackup Terms**.

Use the scroll function to navigate through the glossary.

Accessibility Features

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the *NetBackup System Administrator's Guide for Windows, Volume I* or the *NetBackup System Administrator's Guide for UNIX, Volume I*.

Conventions

The following conventions apply throughout the documentation set.

Product-Specific Conventions

The following term is used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

- Microsoft Windows, Windows

Terms used to describe a specific product or operating system developed by Microsoft, Inc. Some examples you may encounter in NetBackup documentation are, Windows servers, Windows 2000, Windows Server 2003, Windows clients, Windows platforms, or Windows GUI.

When Windows or Windows servers is used in the documentation, it refers to all of the currently supported Windows operating systems. When a specific Windows product is identified in the documentation, only that particular product is valid in that instance.

For a complete list of Windows operating systems and platforms that NetBackup supports, refer to the *NetBackup Release Notes for UNIX and Windows* or go to the VERITAS support web site at `http://www.support.veritas.com`.

Typographical Conventions

Here are the typographical conventions used throughout the manuals:

Conventions

Convention	Description
GUI Font	Used to depict graphical user interface (GUI) objects, such as fields, listboxes, menu commands, and so on. For example: Enter your password in the **Password** field.
Italics	Used for placeholder text, book titles, new terms, or emphasis. Replace placeholder text with your specific text. For example: Replace *filename* with the name of your file. Do *not* use file names that contain spaces. This font is also used to highlight NetBackup server-specific or operating system-specific differences. For example: *This step is only applicable for NetBackup Enterprise Server.*
`Code`	Used to show what commands you need to type, to identify pathnames where files are located, and to distinguish system or application text that is displayed to you or that is part of a code example.
Key+Key	Used to show that you must hold down the first key while pressing the second key. For example: Ctrl+S means hold down the Ctrl key while you press S.

You should use the appropriate conventions for your platform. For example, when specifying a path, use backslashes on Microsoft Windows and slashes on UNIX. Significant differences between the platforms are noted in the text.

Tips, notes, and cautions are used to emphasize information. The following samples describe when each is used.

Tip Used for nice-to-know information, like a shortcut.

Note Used for important information that you should know, but that shouldn't cause any damage to your data or your system if you choose to ignore it.

Caution Used for information that will prevent a problem. Ignore a caution at your own risk.

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

`command arg1|arg2`

In this example, the user can use either the *arg1* or *arg2* variable.

Navigating Multiple Menu Levels

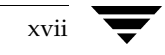
When navigating multiple menu levels, a greater-than sign (>) is used to indicate a continued action.

The following example shows how the > is used to condense a series of menu selections into one step:

❖ Select **Start** > **Programs** > **VERITAS NetBackup** > **NetBackup Administration Console**.

The corresponding actions could be described in more steps as follows:

1. Click **Start** in the task bar.
2. Move your cursor to **Programs**.
3. Move your cursor to the right and highlight **VERITAS NetBackup**.
4. Move your cursor to the right. First highlight and then click **NetBackup Administration Console**.



Introducing NetBackup NetWare Media Server Option 1

This section provides an overview of the NetBackup NetWare Media Server Option and its features.

Introducing NetBackup NetWare Media Server Option includes the following topics:

Section	Describes
"About NetBackup NetWare Media Server Option" on page 1	An overview of the NetWare Media Server Option, how it works in conjunction with NetBackup and NetBackup for NDMP, and introduces some of the terminology used with this application.
"NetBackup NetWare Media Server Option Features" on page 3	The features that are offered by the NetWare Media Server Option.

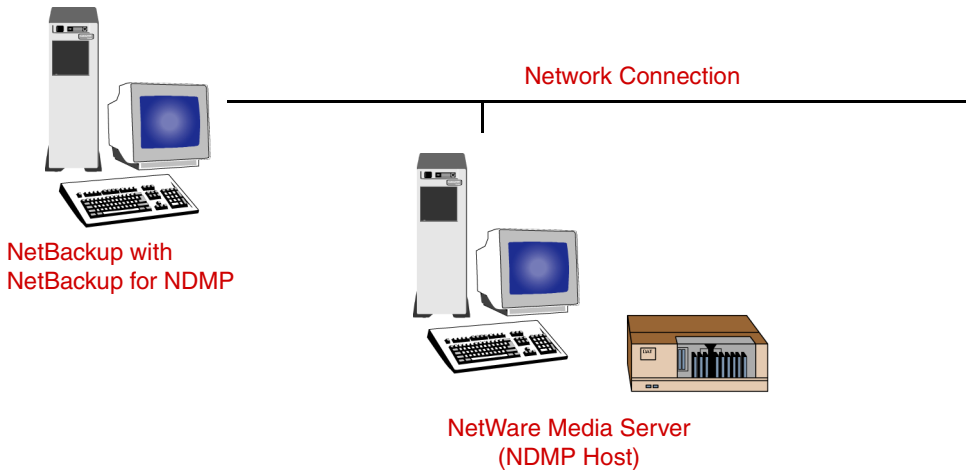
About NetBackup NetWare Media Server Option

NetBackup NetWare Media Server Option is a separately purchased option for VERITAS NetBackup that provides a NetWare media server for NetBackup. With the NetWare Media Server Option, you can control backups and restores of the NetWare media server from a central NetBackup server, but the storage devices used for these backups and restores are attached locally to the NetWare server.

The NetBackup master or media server uses the Network Data Management Protocol (NDMP) to control the backups and restores on the NetWare server, which serves as an *NDMP host*. The host is considered a client of NetBackup, but NetBackup client software is not installed on an NDMP host.

Instead, the NetWare Media Server Option performs backups and restores of the NetWare server as directed by commands that it receives from NetBackup.

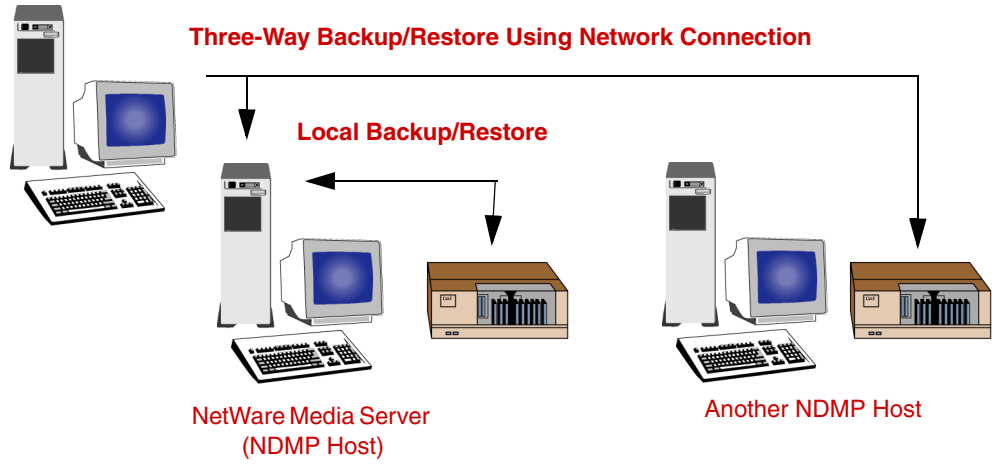
NDMP Architecture Using NetWare Media Server Option



The backup or restore can be a *local* backup or restore, in which the data travels from the NetWare media server to its locally attached storage devices, such as tape drives or robotic libraries. Or, the data can travel over the network between the NetWare media server and a storage device attached to another NDMP host in what is known as a *three-way* backup or restore.

Local Versus Three-Way Backups and Restore

NetBackup with
NetBackup for NDMP



The NetWare Media Server Option includes the Open File Backup Option and Intelligent Disaster Recovery (IDR) options. With the Open File Backup Option, you can back up files that are in use without having to first lock those files. The Intelligent Disaster Recovery option is a fully-automated disaster recovery solution that allows you to quickly and efficiently recover your computers after a disaster.

NetBackup NetWare Media Server Option Features

NetBackup NetWare Media Server Option includes the following features:

- *High speed local backup of a NetWare media server.* Backup data travels between disk and tape drives attached directly to the same NetWare media server, providing high-speed backup without increasing network traffic.
- *Centralized backup policy management*. You can manage backup tasks, such as scheduling jobs and managing catalogs from a NetBackup master server.
- *Device and media management*. NetBackup Media Manager provides total management and control of the devices and media used for backups and restores of NetWare media servers.
- *Shared robots*. You can share robots between NetWare media servers and NetBackup servers or between multiple NetWare media servers. Robotic control can be on an NetWare media server or on a NetBackup server. If the robot is a tape library DLT (TLD) or tape library 8MM (TL8) robot, some of the tape drives can attach to NetWare media servers and other drives can attach to NetBackup servers.

- *Cluster support.* The NetWare Media Server Option supports clustering. With NetWare 6, you can select a virtual server for the backup, and the cluster volume will always be protected. If you are running NetWare 5, the NetWare Media Server option offers two ways of protecting volumes on a cluster. In both cases, you create backup jobs through NetBackup for each node in the cluster. For more information about running the NetWare Media Server Option in a cluster, see "Using the NetWare Media Server Option With a Cluster" on page 41.

Installing the NetBackup NetWare Media Server Option 2

This section explains how to install the NetBackup NetWare Media Server Option and the Open File Backup and Intelligent Disaster Recovery options that come with it. This section also describes the installation requirements.

Installing the NetBackup NetWare Media Server Option includes the following topics:

Section	Describes
"Installation Requirements" on page 5.	Provides the minimum requirement for installing this option and steps for verifying the amount of memory on the media server.
"Installing NetBackup NetWare Media Server Option" on page 7.	Provides steps for installing this option.

Installation Requirements

Before you install NetBackup NetWare Media Server Option, be sure that your media server meets the following minimum requirements:

- Novell NetWare 5.1, 6.0, and 6.5

Note Because the versions of NetWare that NetBackup supports change over time, you should always check the Operating System Compatibility List at http://www.support.veritas.com. By selecting the appropriate version of NetBackup and the Compatibility tab, you will be able to select and view this list.

- 8 MB RAM over server requirements
- 30 MB disk space
- Compatible tape device and controller
- TCP/IP

Note If you are using a Unix master server, you install the VERITAS NetBackup NDMP Option from the options CD to your master server *before* configuring your NetWare media server.

Verifying the Amount of Memory on the Media Server

NetBackup requires a minimum of 8 MB of memory above the standard NetWare memory requirements. The amount of memory required increases as you add more tape devices. If you do not have the minimum amount of memory required when you install NetBackup NetWare Media Server, your system performance will suffer.

▼ **To verify that the Media Server has sufficient memory to install NetBackup NetWare Media Server Option:**

1. At the server console, type **`load MONITOR.NLM`**.
2. Press Enter.
3. Select **System Resources**.

Note If you are using a version of NetWare prior to 5.x, select **Resource Utilization**.

The Server Memory Statistics dialog box displays. If the number next to **Cache buffers memory** is less than 65%, the memory is too low. To increase this number, unload some NLMs that may be using a large amount of memory or add more memory to the server before you install NetBackup NetWare Media Server Option.

Installing NetBackup NetWare Media Server Option

Install NetBackup NetWare Media Server Option from a Windows workstation to each server you want to protect.

▼ **To install NetBackup NetWare Media Server Option:**

1. Insert the installation CD into the Windows workstation's CD-ROM drive.
2. From the installation CD browser, select **Additional Products**.
3. Select **Additional Products Installations**.
4. Select **NetWare Media Server**.
5. Select the language for this install, and then click **OK**.

   The Welcome window appears.
6. Click **Next** to proceed with the installation.

   The License Agreement window appears.
7. Read the license agreement, and then select **I accept the terms of the license agreement**.
8. Click **Next**.
9. Select the options you want to install. Your choices are:
   - **NetBackup NetWare Media Server Option**. Select this option to install the NetBackup NetWare Media Server Option to the server you select.
   - **Open File Backup Option**. Select this option to back up files that are in use without having to lock the files during the backup.
   - **Intelligent Disaster Recovery**. Select this option to install the Intelligent Disaster Recovery option, which allows you to restore a NetWare server in its entirety.
10. Click **Next**.
11. If the NetWare server on which you want to install the files appears in the **Available Servers** list, select the server, and then click the right arrow to move it to the **Destination Systems** list.

    If the NetWare server does not appear in the list, click **Manually add additional systems**, and then type the name of the server.

Note Only one server at a time can be selected as the Destination System.

12. Click **Next**.

Note The server icon in **Destination Systems** displays green if you are connected. If you are not connected, the icon displays red.

13. If you are already connected to the server, click **Next**.

If you are not connected to the server:

a. Click the server's icon in **Destination Systems**.

b. Type the user name and password.

c. Click **Connect**.

d. Click **Next**.

14. Select the installation volume and path, and then click **Next**.

15. If you are satisfied with the settings that display, click **Next**.

If you are not satisfied with the settings, click **Back** until you reach the information you want to change.

The files are copied to *server name*\sys\VERITAS\NBU.

16. If you want the NetBackup NetWare Media Server to load automatically when the server starts, click **Yes**; otherwise, click **No**.

17. Click **Finish** to view the ReadMe file.

18. Click **Exit**.

Setting Up the Account Name and Password

When NetBackup is first started, a default user name and password is created. If you do not want to use this account, you can create your own account name and password. You only have to set up the account and password once.

Note When setting up the NDMP account name, you must provide a *fully distinguished* name, such as .admin.novell. A fully distinguished, or complete, name consists of different object types, such as common name (CN), Organizational Unit (OU) objects, and Organization (O) objects.

▼ **To set up the account name and password on the server:**

1. On the server console type **`load NDMPD -a`** followed by the account name and the name of the context where the account name resides in the directory tree and **`-p`** followed by the password.

   Example: `load ndmpd -a.admin.veritas -padmin`

2. Press Enter.

   The setup is complete. You can now start the NetBackup NetWare Media Server Option.

Starting NetBackup NetWare Media Server Option

▼ **To start NetBackup:**

1. From your system console prompt, type:

   `nbustart`

Note The first time you type **`nbustart`** you will be prompted for user credentials.

2. Press Enter.

Configuring NetBackup for the NetWare Media Server Option 3

This section provides the steps for obtaining information from the NetWare server that will be used when configuring drives, robots, storage units, and policies used for protecting the NetWare media server. This section also describes the steps for granting NetBackup access to the NetWare media server, and for setting up NetBackup to use the NetWare Media Server Option.

Configuring the NetBackup NetWare Media Server Option includes the following topics:

Section	Describes
"Obtaining Device, File System, and Host Information" on page 11	How to display and print device, file system, and host information that must used in NetBackup when setting up policies and storage units for the NetWare media server.
"Providing Access to the NDMP Host" on page 12	The procedures for authorizing the NetBackup media server with access to the NetWare media server.
"Adding Devices, Storage Units, and Policies" on page 16	How to set up NDMP storage devices, storage units, and policies for NetBackup to use for automatic backups of the NetWare server data.

Obtaining Device, File System, and Host Information

Device, file system, and host information for your NetWare media server is needed when setting up storage units and policies in NetBackup for protecting the NetWare data.

▼ **To obtain device, file system, and host information:**

1. On the NetWare server's System Console, type:

   `ndmpcfg`

2. Press Enter.

The information displays on the screen and is also placed in a file called `ndmpconfig` in the root directory of the volume (`SYS:\`).

3. Navigate to `SYS:\` and print the `ndmpcfg.log` file.

Keep the print out on hand while you set up access to the NDMP host, and set up devices, storage units, and policies.

Providing Access to the NDMP Host

For the NetBackup media server to control backups and restores on the NetWare media server, you must first provide the NetBackup master server access to the NetWare NDMP host. To provide this access, you must add the NDMP host information to the NetBackup master server's Hosts file, and then authorize access to the NDMP host. If robotic libraries are attached to the NetWare media server, you must configure robotic control by specifying the device name, controller number, SCSI ID, and LUN (logical unit number) on the NetBackup master server before verifying access to the NDMP host.

Adding the NDMP Host Information to the Hosts File

If you are not using Domain Name Services (DNS), then the IP addresses for the NetWare servers you want to communicate with must be included in the NetBackup master server's Hosts file.

▼ **To add your NetWare server's address to the NetBackup Server's Hosts file:**

1. Open the Hosts with a text editor, such as Notepad.

2. On a blank line, type the IP address of the NetWare server, followed by at least one space, and then the server's name.

3. Save the Hosts file.

Note The Hosts file should *not* have a file name extension.

Authorizing Access to the NDMP Host

Before you can use NetBackup for backup or restore operations on the NetWare media server, you have to provide NetBackup with access to the NDMP host. If you plan to run three-way backups, you must provide access to both the NDMP host that does not have a storage device attached to it as well as the NDMP host with the storage devices attached.

Note If you have not entered the IP address for your NDMP host in the Hosts file of your workstation, you must enter the IP address rather than the NDMP host name.

If you are using a Unix master server, you install the VERITAS NetBackup NDMP Option from the options CD to your master server *before* configuring your NetWare media server.

▼ **To authorize access to the NDMP host:**

1. On a DOS command line on the NetBackup master server on a Windows computer, type:

   install_path\Volmgr\bin\set_ndmp_attr -auth *ndmp_host user_name*

   For a a UNIX computer, type:

   install_path/Volmgr/bin/set_ndmp_attr -auth *ndmp_host user_name*

Note The default install path for a Windows computer is C:\Program Files\Veritas; for a a UNIX computer, the default install path is /usr/openv/.

NDMP_host is the name of the NDMP host that NetBackup will be backing up. *User_name* is the user name under which NetBackup will access the NDMP host. This user must have persmission to execute the NDMP commands.

In the following example, *C:\Program Files* is the install path, *darva* is the NDMP_host, and *admin* is the user_name.

C:\Program Files\Volmgr\bin\set_nmdp_attr -auth darva admin

You will be prompted to enter the password twice. The default NetWare Media Server Option password is **bex**.

2. Type **bex**, and then press Enter.

3. Re-type **bex**, and then press Enter.

   Typing bex authorizes the use of the NetWare Media Server Option by NetBackup.

Configuring Robotic Control

If your NetWare media server has robotic libraries attached, you must configure robotic control using the `set_ndmp_attr -robot` command.

Note If you are using a Unix master server, you install the VERITAS NetBackup NDMP Option from the options CD to your master server *before* configuring your NetWare media server.

▼ **To configure robotic control:**

❖ On a DOS command line on the NetBackup master server on a Windows computer, type:

install_path\Volmgr\bin\set_ndmp_attr -robot *NDMP_host robot_device scsi_controller scsi_id scsi_lun*

For a a UNIX computer, type:

install_path/Volmgr/bin/set_ndmp_attr -robot *NDMP_host robot_device scsi_controller scsi_id scsi_lun*

Note The default install path for a Windows computer is C:\Program Files\Veritas; for a a UNIX computer, the default install path is /usr/openv/.

NDMP_host is the name of the NetWare media server serving as the NDMP host to which the robotic library is attached.

Robot_device is the device name for the robot.

SCSI_controller is the controller number.

SCSI_ID is the SCSI ID for the robot.

SCSI_lun is the LUN for the robot.

After all configurations have been entered for all robots attached to your NetWare media server, you can list your configuration settings by again typing the set_ndmp_attr command followed by the -list option. For example, if your NetBackup media server is a Windows computer, you would type:

install_path\Volmgr\bin\set_ndmp_attr -list

Note If you change the robot configuration on the NDMP host, use `set_ndmp_attr -robot` to update the NetBackup master server with your changes.

Verifying Authorization

After you have entered the authorization and configured robotic control for all libraries attached to your NetWare media server, verify that the NetBackup master server can connect to the NDMP host.

▼ **To verify connection to the NDMP host:**

❖ On a DOS command line on the NetBackup master server on a Windows computer, type:

install_path\Volmgr\bin\set_ndmp_attr -verify *NDMP_host*

For a a UNIX computer, type:

install_path/Volmgr/bin/set_ndmp_attr -verify *NDMP_host*

Note The default install path for a Windows computer is C:\Program Files\Veritas; for a a UNIX computer, the default install path is /usr/openv/.

Verifying Host Connection

```
C:\Program Files\VERITAS\Volmgr\bin>set_ndmp_attr -verify darva
Connecting to host "darva" as user "admin"...
Waiting for connect notification message...
Opening session--attempting with NDMP protocol version 3...
Opening session--successful with NDMP protocol version 3
  host supports MD5 authentication
Getting MD5 challenge from host...
Logging in using MD5 method...
Host info is:
  host name "DARVA"
  os type "NetWare"
  os version "v5.0"
  host id "6932430a"
Login was successful
Host supports LOCAL backup/restore
Host supports 3-way backup/restore
Opening SCSI device "/dev/scsi/_00_05_00"...
Setting SCSI target controller 0 id 5 lun 0...
Inquiry result is "ADIC    FastStor DLT    D18A"

C:\Program Files\VERITAS\Volmgr\bin>
```


Adding Devices, Storage Units, and Policies

For NetBackup to use the NetWare Media Server Option to launch backups on the NetWare media server, you must first create for each NDMP host:

- Storage devices (see "Adding NDMP Storage Devices" on page 16)
- Storage units (see "Creating NDMP Storage Units" on page 21)
- Policies (see "Creating NDMP Policies" on page 24)

These are created from the NetBackup master server using the information you obtain from your NetWare media server (see "Obtaining Device, File System, and Host Information" on page 11).

Adding NDMP Storage Devices

You must use Media Manager to add the drives and robots that attach to the NDMP host before NetBackup can use them as storage devices and before you can create a storage unit for these devices (see "Creating NDMP Storage Units" on page 21).

▼ To add a robot attached to an NDMP host:

1. If the NetBackup master server is a Windows computer, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration Console**.

   If the NetBackup master server is a UNIX computer, type:

   /usr/openv/netbackup/bin/jnbSA &

2. From the left pane of the NetBackup Administration Console window, click **Devices**.

Note If you are not running NetBackup Administration Console on the NetBackup master server, use the **Monitor** command on the **Hosts** menu to switch to the NetBackup master server.

3. Click **Actions** menu, select **New**, and then select **New Robot**.

4. Complete the options for the Add Robot dialog box. The options are described in "Add Robot Dialog Box" on page 18.

5. Click **OK**.

6. If you have additional robots or drives to add, click **No** when prompted if you want to stop and restart the NetBackup Device Manager service. When all robots and drives have been added, click **Yes** on this prompt.

▼ To add a drive attached to the NDMP host:

1. If the NetBackup master server is a Windows NT/2000 computer, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration Console**.

   If the NetBackup master server is a UNIX computer, type:

   /usr/openv/netbackup/bin/jnbSA &

2. From the left pane of the NetBackup Administration Console window, click **Devices**.

Note If you are not running NetBackup Administration Console on the NetBackup master server, use the **Monitor** command on the **Hosts** menu to switch to the NetBackup master server.

3. From the **Actions** menu, select **New**, and then select **New Drive**.

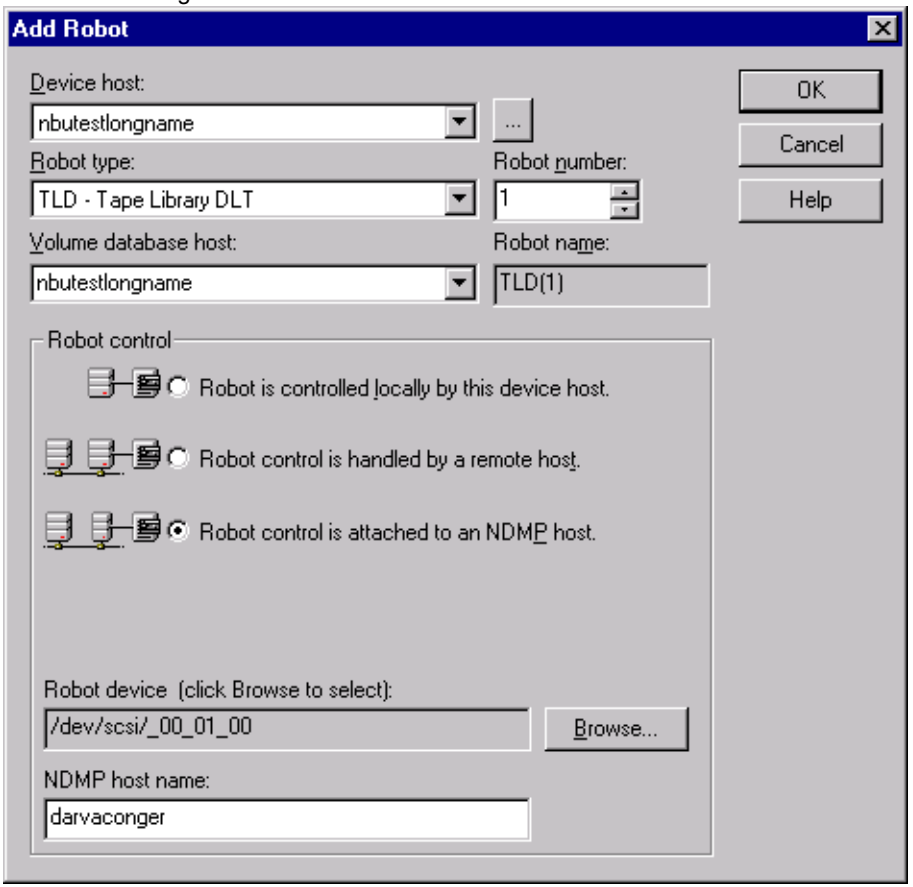
4. Complete the options for the Add Drive dialog box. The options are described in "Add Drive Dialog Box" on page 20.

5. Click **OK**.

Add Robot Dialog Box

The Add Robot dialog box allows you to enter information about robots attached to your NetWare server.

Add Robot Dialog Box



Options on this dialog include:

- **Device host**. Specify the Media Manager host to which you are adding the robot. The host shown by default is the device host you selected earlier in the tree. If you want to specify a different host, select a name from the list, or use the browse button to select a host not appearing in the list.
- **Robot type**. Select the type of robot you are adding.
- **Robot number**. Specify a unique, logical identification number for the robot. This number identifies the robot in listings, such as Robot 1 - TLD. You also use this number when adding the robot's media to the Media Manager configuration. Robot

numbers must be unique for all physically-distinct robots on all hosts in the configuration, regardless of the robot type or the host that controls them. For example, there cannot be two robots with robot number 1, even if the robots are controlled by and configured on different hosts. If you are adding a robot definition for a robot controled by a remote device host, be sure to use the same robot number for that robot on all other device hosts.

- **Volume database host**. Specify the name of the host where Media Manager keeps the volume configuration information about the media in the robot. You must know the name of the volume database host when adding volumes to the robot. You can specify any Media Manager host as the volume database host, even if the host does not have any attached drives or robots.

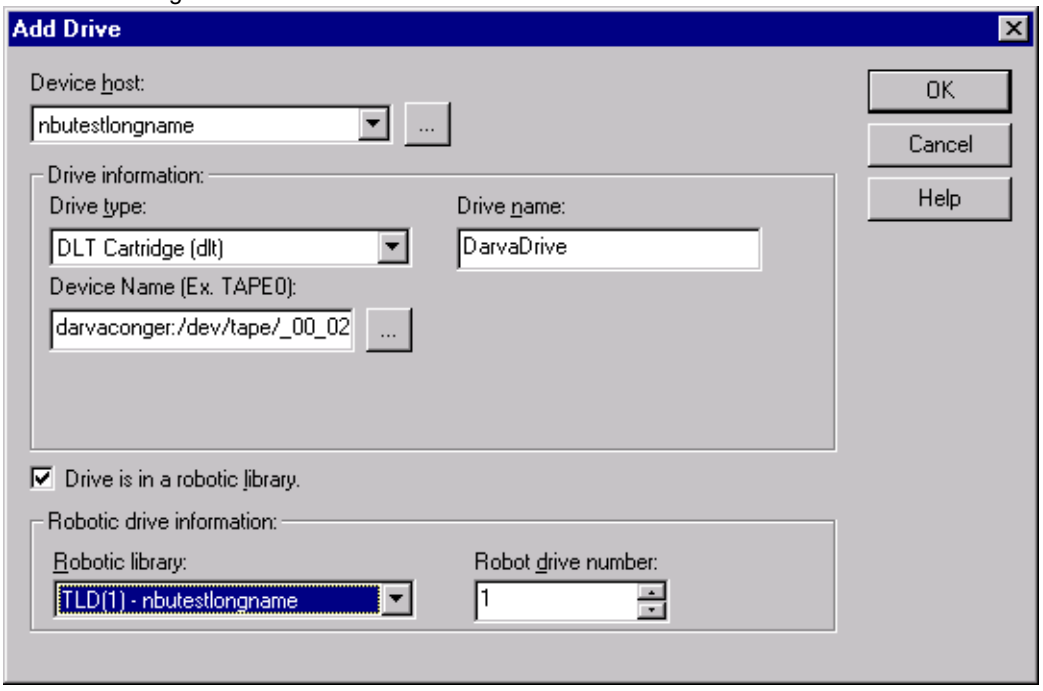
Caution It is recommended that you use one volume database host for all your volumes (robotic and stand-alone drives). Although it is possible to maintain separate volume databases on multiple hosts, administration is more difficult and it is not possible to merge databases.

- **Robot control**. Select the option **Robot control is attached to an NDMP host**.
- **Robot device**. Click **Browse**, and then specify the controller number, SCSI ID, and SCSI LUN information for the robot device that is attached to the NDMP host. This information can be obtained on the SCSI section of the NDMPCFG printout (see "Obtaining Device, File System, and Host Information" on page 11).
- **NDMP host name**. Enter the name of the NetWare media server.

Add Drive Dialog Box

The Add Drive dialog box allows you to enter information about the drives attached to your NetWare server.

Add Drive Dialog Box



Options on this dialog box include:

- **Device host**. Specify the Media Manager host to which you are adding the drive. The host shown by default is the device host you selected earlier in the tree. If you want to specify a different host, select a name from the list, or use the browse button to select a host not appearing in the list.
- **Drive type**. Specify the type of drive you are adding.
- **Drive name**. Enter the name that will be used by the Media Manager to identify the drive. Descriptive names are recommended.
- **Device name**. Name of the physical device on the NetWare computer preceded by the host name and a colon. This information can be obtained on the Tape section of the NDMPCFG printout (see "Obtaining Device, File System, and Host Information" on page 11).
- **Drives is in a robotic library**. Select this option if the drive is in a robotic library. Clear this option if the drive is a stand-alone drive.

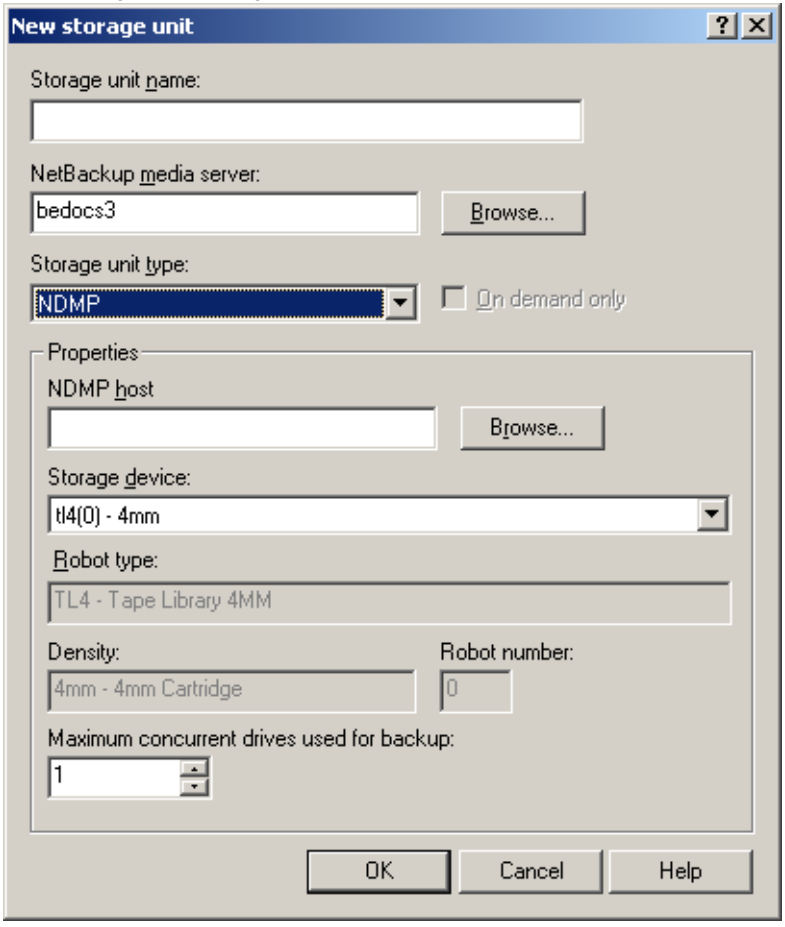
- **Robotic library**. If **Drive is in a robotic library** is selected, select the robot that controls the drive. If the robotic library does not appear in the drop-down list, it has not yet been added.
- **Robot drive number**. Select the robot drive number assigned to this drive.

Creating NDMP Storage Units

An NDMP storage unit consists of one or more storage devices of a specific type and density that are attached to an NDMP host but are controlled by NetBackup's Media Manager. NetBackup stores data on these storage units during a backup of the NDMP host. Before setting up storage units, add the robots and devices that will be used by the NDMP host through the Media Manager (see "Adding Devices, Storage Units, and Policies" on page 16).

Refer to the *VERITAS NetBackup System Administrator's Guide for Windows* or the *VERITAS NetBackup System Administrator's Guide for UNIX* for the procedures for creating the storage units.

New Storage Unit Dialog



Enter the following options on the **New Storage Unit** dialog:

- **Storage Unit Name**. Type a unique name that describes the storage unit you are defining. Use alphabetic, numeric, plus, minus, underscore, or period characters. Do not use a minus as the first character or leave spaces between characters. The storage unit name, which is to be used when specifying a storage unit for policies or schedules, cannot be changed after creation.
- **NetBackup media server**. Defaults to the name of the local NetBackup master server that will control backups for the NDMP media host.
- **Storage unit type**. Select NDMP from the drop-down list.
- **On demand only**. Select this option if the storage unit is to be available only when a policy or schedule requests it; otherwise, the storage unit is available to any NDMP policy or schedule. Select this option if both of the following conditions exist:

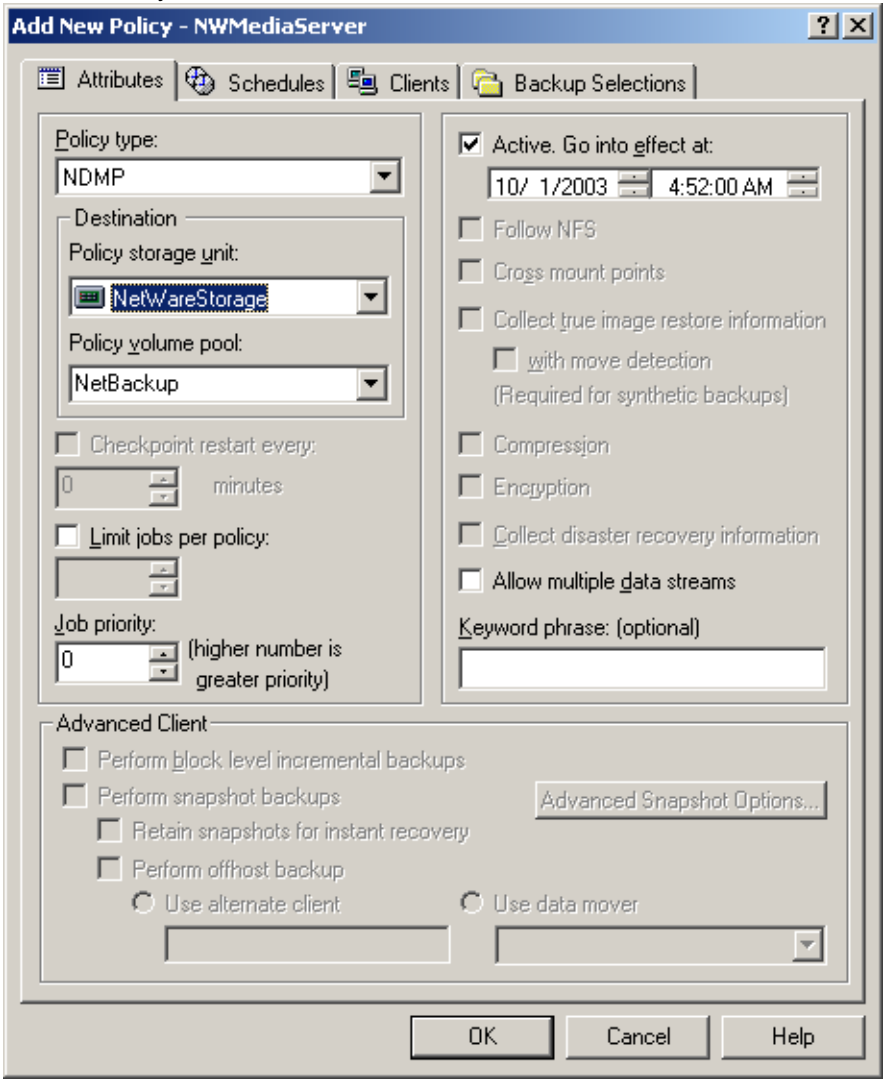
- The NDMP host with the storage unit is the only one in the policy.
- There is more than one storage unit for the NDMP host, and you want to use the storage units for specific schedules. For example, you can set up schedules to use one storage unit for full backups while another storage unit is set up use with incremental backups.

- **NDMP host**. Enter or use **Browse** to select the name of the NetWare media server.
- **Storage device**. Select a device from the drop-down list. Storage units can be created for listed devices only.
- **Robot type**. Select the type of robot (if any) that the storage unit contains, or if the device is a stand-alone drive, select **NONE - Not Robotic**.
- **Robot number**. For a robotic storage unit, this is the same robot number used when adding the robot.
- **Density**. Specify the media density that the storage unit will use.
- **Maximum concurrent drives used for backup**. Specify the number of drives that NetBackup can use at one time for backups using this storage unit. The number cannot be more than the total number of drives assigned to this storage unit.

Creating NDMP Policies

The backup policy that sets rules for backing up the NDMP host must be created on the NetBackup master server following the procedures outlined in the *NetBackup System Administrator's Guide* (Windows NT/2000 or UNIX).

Add New Policy - Attributes Tab

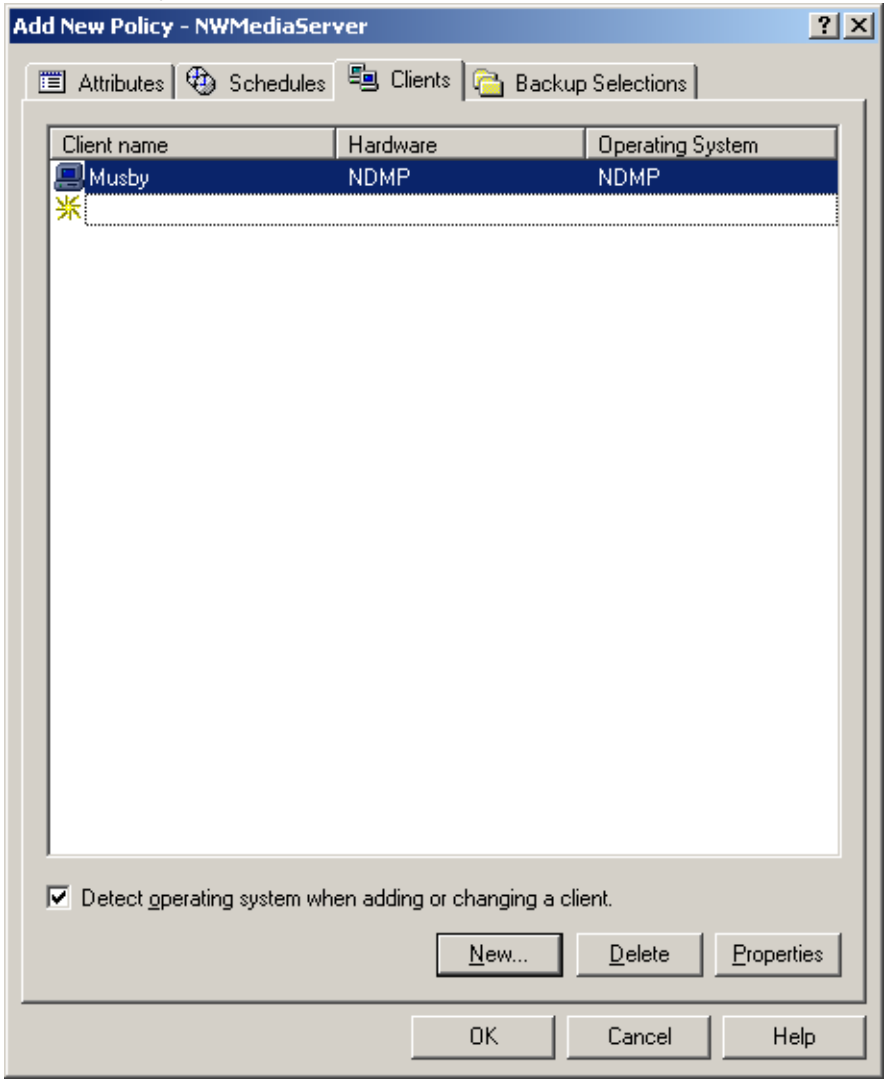


For the NetWare Media Server Option, specify the following policy attributes:

- **Policy type**. Select NDMP from the drop-down list of policy types. Policy type determines the type of clients that can be protected by this policy.

- **Policy storage unit**. Specify the name of the storage unit that will be used for this policy. For local backups, the Policy storage unit must be attached to the NDMP host. For three-way backups, you can specify a storage unit on another NDMP host.

Add New Policy - Clients Tab



In the client list, specify the following for each client in an NDMP policy:

- **Client name**. Enter the name of the NetWare server.
- **Hardware and operating system**. Select NDMP NDMP.

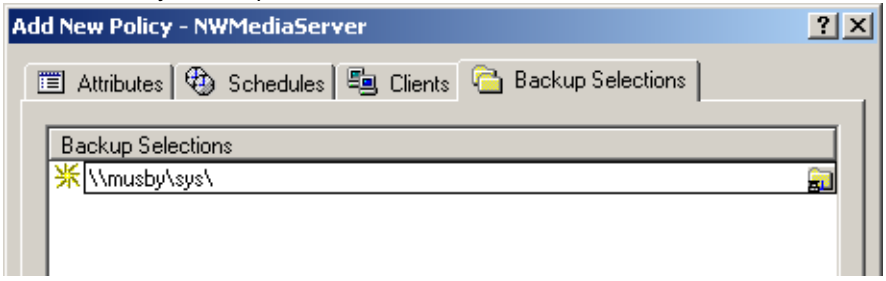
When selecting the files to be automatically backed up, provide the directory name as part of the file. For example, *NDMP host*\sys\logs\. Wildcards cannot be used in pathnames for an NDMP policy, and you cannot provide an **Exclude list**, although you can use the **SET** option as an environmental variable to exclude files on a backup.

Using Environmental Variables in a Selections List

On the **Add New Policy - Selections** tab, you can use environmental variables to pass configuration parameters to the NetWare media server with each backup and restore. NDMP environmental variables can include variables that are:

- Defined as optional by the NDMP specification.
- Specific to an NDMP host vendor.

Add New Policy - Backup Selections Tab



Variables reserved for use by NetBackup include:

- FILESYSTEM
- LEVEL
- DIRECT
- EXTRACT
- ACL_START

You can set variables defined as option by NDMP or specific to an NDMP host vendor by specifying one or more SET directives, using the following syntax:

```
SET variable = value
```

Variable is the name of the environment variable and value is the value assigned to the variable. The value can be enclosed in single or double quotes, and must be enclosed in quotes if it contains a space character.

Setting a variable equal to no value removes the variable. For example:

```
SET ABC =
```

Note The set command entry must occur in the file list before the directories and files to which it applies.

Variables accumulate as the file list is processed. For example, suppose the file list contains the following entries:

```
SET HIST = N
\\NDMP Host\SYS\
SET HIST = Y
\\NDMP Host\USER\
```

The entire SYS volume would be backed up without sending any file history. The USER volume would then be backed up and file history information would be sent.

If an environment variable appears again in the list, the second value listed overrides the previous value of the variable.

The values used in each backup are saved and provided to subsequent restores of the directory. The NDMP host may have environment variables that are set internally; these are also saved for restores.

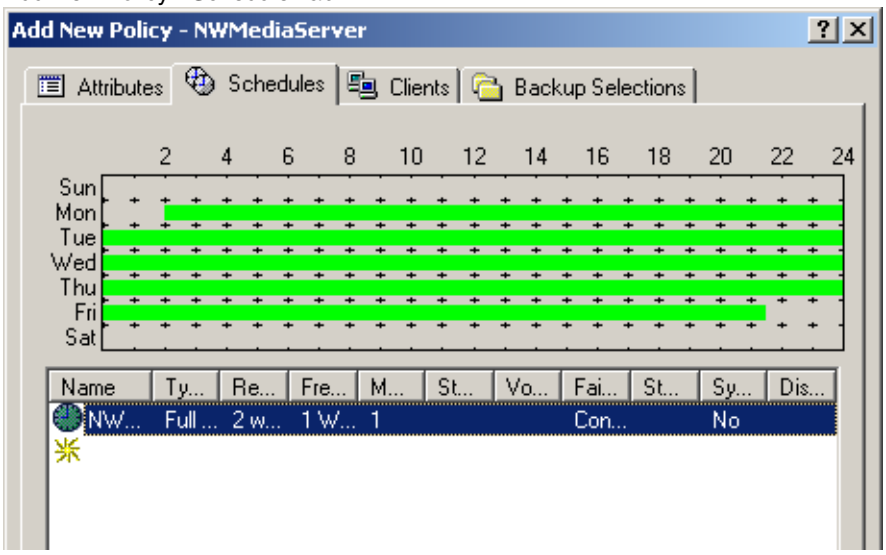
The type of data that can be backed up on the server will be listed in the NDMPCFG file, along with the syntax required for entering this information. For example:

*****server name***\Server Specific Info**

Setting Schedules

The schedule for your NDMP backup is set in the **Add New Policy - Schedule** tab.

Add New Policy - Schedule Tab



You can select any of the following backup types in a schedule for an NDMP policy:

- **Full**. Backs up all files in the file list for the policy, regardless of when they were last modified or backed up. If you use incremental backups, you must also schedule full backups to perform a complete restore.
- **Cumulative Incremental**. Backs up all files in the file list that have changed since the last successful full backup. All files are backed up if no prior backup was done. When this backup type is used, a complete restore of your computer requires the last full and the last cumulative incremental backup.
- **Differential Incremental**. Backs up all files in the file list that changed since the last incremental or full backup. When this backup type is used, a complete restore of your computer requires the last full backup and all differential backups made since the last full backup.

Specify **Override policy storage unit** only if the NetWare server has more than one storage unit and you want to use a specific storage unit for this schedule. The NetWare server must be the only client in the NDMP policy.

Using the NetWare Media Server Option 4

This section explains how to create manual backups of and restore data to the NetWare server using NetBackup and the NetWare Media Server Option. This section also addresses how to use the Open File Backup Option included with the NetWare Media Server Option.

Using the NetWare Media Server Option includes the following topics:

Section	Describes
"Performing a Backup" on page 30	How to create a backup job using the NetWare Media Server Option.
"Performing a Restore" on page 31	How to restore data using the NetWare Media Server Option.
"Using the Open File Backup Option" on page 33	How to protect open files using the Open File Backup Option and the NetWare Media Server Option.
"Using the NetWare Media Server Option With a Cluster" on page 41	How to use the NetWare Media Server Option to protect data in a cluster environment.

Performing a Backup

User-directed backups of the NetWare system serving as the NDMP host are not permitted. Instead, backups can either be created automatically or manually by the administrator on a NetBackup server. Automatic, unattended backups are created by NetBackup based on the creation of policies and schedules (see "Creating NDMP Policies" on page 24 and "Setting Schedules" on page 28).

You cannot back up files where the path length is greater than 1024 characters. You can only include directory or volume paths and cannot use wildcards in the file list for an NDMP policy.

▼ To create a manual backup of an NDMP policy:

1. If the NetBackup for NDMP server is a Windows computer, click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **NetBackup Administration Console**.

   If the NetBackup for NDMP server is UNIX computer, type:

   ```
   /usr/openv/netbackup/bin/jnbSA &
   ```

2. Click the NDMP policy name in the left pane.

3. From the **Actions** menu, select **Manual Backup**.

4. On the Manual Backup dialog, select the schedule and the NDMP hosts (Clients) that you want to back up.

   If you do not select a schedule, NetBackup uses the schedule with the highest retention level. If you do not select an NDMP host, NetBackup backs up all NDMP hosts.

5. Click **OK**.

Performing a Restore

User-directed restores are not allowed. Instead, the administrator can restore files to the NDMP host from which they were backed up by creating a restore job from the NetBackup server. Files backed up from an NDMP storage unit cannot be restored from a non-NDMP storage unit.

Caution An NDMP restore always overwrites existing files.

▼ To perform a restore from a Windows NetBackup server:

1. Click **Start**, point to **Programs**, point to **VERITAS NetBackup**, and click **Backup, Archive, and Restore**.
2. From the Backup, Archive, and Restore window, click **Select for Restore** from the tool bar.
3. From the **File** menu, click **Specify NetBackup Machines and Policy Type**.

   The Specify NetBackup Machines and Policy Type dialog appears. Modifications made in this dialog affect all open restore windows and are not saved after closing the Restore window.
4. On the **Servers** tab, specify the NetBackup master server. If your configuration has multiple master servers, specify the master server that has the policy for the NDMP host you are restoring.
5. Click **Make Current**.
6. On the **Source Clients/Policy Type** tab, specify the NetWare server on which the storage unit is attached.
7. In the **Policy Type** field, select **NDMP**.
8. On the **Destinations Clients** tab, select the NetWare server you want to restore to, click **Make Current**, and then click **OK**.
9. On the Restore window, browse and mark the files and folders you want to restore.
10. From the **Actions** menu, click **Start Restore of Marked Files**.
11. Complete the options on the Restore Marked Files dialog.
12. Click **Start Restore**.

▼ To perform a restore from a UNIX NetBackup server:

1. Type:

   ```
   /usr/openv/netbackup/bin/jnbSA &
   ```

2. Click the **Backup, Archive, and Restore** node.

   The Backup, Archive, and Restore window appears. Modifications made in this window affect all open restore windows and are not saved after closing the restore window.

3. From the **Action** menu, select **Specify NetBackup Machine**.

4. On the **NetBackup server** tab, specify the NetBackup master server. If your configuration has multiple master servers, specify the master server that has the policy for the NDMP host you are restoring.

5. On the **Source client** tab, specify the NetWare server on which the storage unit is attached.

6. In the **Policy Type** field, select **NDMP**.

7. On the **Destination client** tab, select the NetWare server you want to restore to.

8. Browse and mark the files and folders you want to restore.

9. Click **Restore**.

10. Complete the options on the Restore Files dialog.

11. Click **Start Restore**.

Using the Open File Backup Option

The Open File Backup Option allows you to back up open files on your NetWare media server serving as the NDMP host. The Open File Backup Option must be installed on the NetWare system along with the NetWare Media Server Option.

After the Open File Backup Option is installed, it runs in the background of the NetWare media server, waiting for a job using this option to run. When a backup job using the Open File Backup Option starts, a point-in-time or static view of the volume is created. This static, unchanging view of the volume is then backed up and released when the backup completes.

The volumes you want to back up with the Open File Backup Option on NetWare 5.x must be traditional NetWare volumes; NetWare 5.x NSS volumes are not supported. NSS volumes are only supported on NetWare 6.x.

During a backup using the Open File Backup Option, if changes are made to the original data, the Open File Backup Option makes a duplicate of the original data before it is changed and stores this duplicate in a buffer.

When the backup is complete, the static volumes are automatically dismounted.

Caution Buffer files should not be manually removed unless all backup activity is done.

In a cluster environment, if the cluster volume joins or leaves the node, a second static view is made. This could affect the integrity of the backup.

Open File Backup Option Requirements

In addition to meeting the installation requirements listed in "Installation Requirements" on page 5, the NetWare media server must also have:

- The Open File Backup Option installed.
- Sufficient free space on the volume containing the cache file. This amount depends on the amount of file changes that occur during a backup; a minimum of 40 MB of free disk space is required after installation.
- Sufficient memory to mount a duplicate of the volumes that are being protected.
- Volumes that are IDE or SCSI devices; I20 and SSA drives are not supported.

The volumes you want to back up with the Open File Backup Option on NetWare 5.x must be traditional NetWare volumes; NetWare 5.x NSS volumes are not supported. NSS volumes are only supported on NetWare 6.0.

Note The Open File Backup Option cannot be used on CD-ROM drives, floppy disk drives, or the media server's DOS partitions.

The volume containing the cache file must have at least 40 MB of available space.

Creating a Backup Job Using the Open File Backup Option

To create a backup job using Open File Backup Option, the policy used for the backup must contain the environmental variable DO_SNAPSHOT=1.

▼ **To set the Open File Backup Option variable:**

1. Select the policy that will be used for this backup.
2. Select the **Selections** tab.
3. Above the list of files that you want backed up using the Open File Backup Option, type:

   ```
   set DO_SNAPSHOT=1
   ```

Note The set command entry must occur in the file list before the directories and files to which it applies.

4. Save the policy, and then complete a backup following the procedures described in "Performing a Backup" on page 30.

Configuring Open File Backup Option Settings

It is strongly recommended that you use the default settings for the Open File Backup Option. However, if you need to modify configuration information, you can use a text editor to edit the following files:

- NetWare System Component Configuration (OFMNW.CFG)
- NetWare NSS Configuration (OFMCDM.CFG)

Some parameters in the two configuration files are for internal use only and should not be modified.

The NetWare NSS Configuration file is located in `SYS:\SYSTEM`. Both the NetWare System Component Configuration file and the NetWare Pass-Through Agent Definitions file are located in `SYS:\SYSTEM\OFM`.

OFMNW.CFG and OFMCDM.CFG have three groups of entries:

- **Comments**. Each line that begins with a semicolon (;) is treated as commentary and is ignored.
- **General**. The marker [General] occurs in each file one time and begins the series of general configuration settings.
- **Group**. The marker [Group] occurs in each file one time and begins the series of Files to Ignore specifications.

In some of these sections are common settings that appear in both configuration files (see "Common Settings for Configuration Files" on page 35. There are also additional parameters in these three sections that appear only in the OFMNW.CFG file (see "Additional Settings for OFMNW.CFG" on page 38) or only in the OFMCDM.CFG file (see "Additional Settings for OFMCDM.CFG" on page 40).

Common Settings for Configuration Files

The common settings or parameters for the OFMNW.CFG and OFMCDM.CFG files include:

Common Parameters for Configuration Files

Parameter	Description
[General]	
BreakOnAssert	For internal use only; do not modify.
BreakOnException	For internal use only; do not modify.
HashBucketCount	For internal use only; do not modify.
LCI	For internal use only; do not modify.
LockContentionLimit	For internal use only; do not modify.
LogFileMaxSize	Specifies the maximum size setting for the system component's log file; for example, 1024.
LogFilePath	Specifies the local location of the system component's log file; for example, `SYS:\SYSTEM\OFM.OFMNW.LOG`.
MinVolFreeSpace	Specifies the default minimum free space requirement for each volume in kilobytes; for example, 4096.

Common Parameters for Configuration Files (continued)

Parameter	Description
PreviewDataReleasePoint	Specifies when data can be previewed. Options are: • 1 - After backup • 2 - After verify • 3 - After all backup activity stops
PreWriteCacheBlockSize	For internal use only; do not modify.
StatusPrintLevel	For internal use only; do not modify.
SyncInactivityTimeout	Specifies the backup inactivity timeout in seconds; for example, 120.
VerboseMsgLogging	Specifies whether or not verbose diagnostic messages are added to the log file and displayed on the NetWare console. The default setting is 0 for `False`. To add verbose diagnostic messages, change this value to 1. Enabling this option could adversely affect performance.
VolDisableOfm	This parameter is part of the support for disabling the Open File Backup Option on some volumes. Instead of modifying this setting directly, you should enter volume specifications in the Group section of the configuration files or in the list of Files to Ignore.
WriteInactivityPeriod	Specifies the write inactivity period in seconds; for example, 5.
[Group]	
GroupUID	Identifies the type of group. This ID should always be 4097.

Common Parameters for Configuration Files (continued)

Parameter	Description
File	Specifies the file or directory to be ignored. The components of this parameter are: • Value of 0x0 or 0x1 to specify whether or not subdirectories should be ignored. This value should be 0x0 (false) for files, but can be 0x1 (true) for directories if the entire directory subtree is to be ignored. • Namespace. This should always be DOS. • Volume and path specification of the file or directory to be ignored. For example, if you wanted to ignore files in a directory called Temp1 but not the files in its subdirectories, the parameter entry in the configuration file would be: **`File=0x0, DOS, SYS:\temp\Temp1\*`** **Note** The line `File=0x1, DOS, SYS:\BKUPEXEC\*` should be added to this section on all server nodes in a cluster, replacing SYS with the name of the cluster volume on which the NetWare Media Server Option is installed.

See also:

"Additional Settings for OFMNW.CFG" on page 38

Additional Settings for OFMNW.CFG

In addition to the common settings described in "Common Settings for Configuration Files" on page 35, there are settings that only pertain to the NetWare System Component Configuration file. These additional settings include:

Additional OFMNW.CFG Settings

Parameter	Description
[General]	
AgentFilePath	Specifies the location of the NetWare System Component's Agent Definition File. For example, `SYS:\SYSTEM\OFM\OFMNW.AGT`.
AgentRecreatesDir	By default, this field is set to 1 for `True` and can be changed to 0 for `False`. Create, Delete, Rename Handling, and NSS directories and files deleted while the system is synchronized will continue to be available to backup applications, and will be fully backed up. However, the directories themselves (but not the files within them) may also be recreated. The result is an empty directory for any directory backed up after it is deleted while the system is synchronized. The AgentRecreatesDir parameter allows you to disable this behavior so that directories deleted while synchronized are not recreated when they are backed up during the same synchronization session. **Note** If AgentRecreatesDir is set to 0, OFO must be unloaded when a restore is performed or directories will not be created during restores.
ConfigFilePath	Specifies the local location of the NetWare System Component's configuration file. The path is fixed, so this value is always the same.
HandleTruncatedFiles	By default, this field is set to 1 for `True` and can be changed to 0 for `False`. This value relates to files that are truncated by another application, while a backup is in progress. A truncated file is one whose content is deleted, but continues to exist as an empty file. A `True` value means that OFO will preserve the content for the backup but that the content will not be available for NetWare Salvage. A `False` value means that the content can be salvaged, but will not be available to the backup.

Additional OFMNW.CFG Settings (continued)

Parameter	Description
IgnoreQDRDirectories	By default, this field is set to 1 for True and can be changed to 0 for False. This value determines whether the queue directories, `SYS:\SYSTEM\*.QDR` and `\QUEUES\*.WDR` on any volume, are included in the predefined list of files to ignore.
MinServerMemory	Specifies the minimum free memory (available RAM) requirement in percent. If the available free memory falls below this percentage, OFO System Component will pause its operation, releasing the memory back to the system to meet demand. The paused System Component must then be manually restarted by unloading and reloading through the NetWare system console.
PauseOnMemFailure	By default, this field is set to 1 for True and can be changed to 0 for False. Normally, OFO disables itself if it detects that the NetWare server is running critically low on available memory. Setting this parameter to 0 overrides this behavior.
PreviewDataVolRes [*volume_name*]	This value overrides the default MinVolFreeSpace setting for the named volume. There may be multiple instances of this setting, each naming a specific volume.
PWCSpaceUsedIncr	Specifies the number of bytes sent from the System Component to the Control Component for each increment. Changing this value to a larger number will cause less network traffic but could provide less accuracy in the Control Component display.
UseEmergencyMemPool	By default, this field is set to 0 for `False` and can be changed to 1 for `True`. When set to 1, an emergency memory pool is allocated to allow continued, degraded operation during sustained stress testing. Changing this parameter is *not* recommended for production environments.
VolumeNoPreview*digit*	The digit (for example, 0) is a distinct digit for each VolumeNoPreview item. This parameter specifies a volume that should not be used for storing Preview Data. For example, if the parameter is `VolumeNoPreview0=SYS`, all volumes will be used for storing preview data except for SYS.

Additional OFMNW.CFG Settings (continued)

Parameter	Description
SynchronousSync	By default, this field is set to 1 for `True` and should not be changed. This parameter controls the behavior of OFO's programmatic Synchronized API. By default, synchronization of LFS volumes will be complete when the API returns. Alternatively, when this parameter is false, the API returns asynchronously. Synchronization of NSS volumes is always complete when the API returns.

Additional Settings for OFMCDM.CFG

In addition to the common settings described in "Common Settings for Configuration Files" on page 35, there are settings that only pertain to the NetWare NSS Configuration file. These additional settings include:

Additional OFMCDM.CFG Settings

Parameter	Description
[General]	
AutoMountVolumes	By default, this field is set to 0 for `False` and can be changed to 1 for `True`. This parameter is the Mount Synchronized Volumes parameter.
BackupCachePoolName	If not empty, this field specifies the name of a pool to use as recourse for pre-write caches; this pool would be used to hold the cache for another pool that does not have sufficient space. The default value is empty, which allows OFO to automatically select the pool with the most free space.
CacheBlockSize	Specifies the unit of size in which NSS data is written to the pre-write cache. Larger values generally provide better performance on busy systems; smaller values consume less space. If the value is too large, synchronization will fail on fragmented pools. The default, which is 0x4000 hex bytes (16 KB), should usually not be exceeded.
CacheLFS	By default, this field is set to 0 for `False` and can be changed to 1 for `True`. This setting controls whether or not to create synchronized LFS volumes. **Note** This feature is currently not supported.

Additional OFMCDM.CFG Settings (continued)

Parameter	Description
GetHamSetStateTimeout	For internal use only; do not modify.
LFSCachePoolName	If CacheLFS is set to `True`, this parameter specifies the name of a pool to use for LFS pre-write caches. It is also used to cache LFS partition headers, regardless of whether or not CacheLFS is set to `True`. The default value is empty, which allows OFO to automatically select the pool with the most free space.
MinServerMemoryPercent	Specifies the minimum percentage of free memory (available RAM) requirement. If the available free memory falls below this percentage, the OFO system component will pause its operation, releasing memory back to the system to meet demand. The paused system component must then be manually restarted by unloading and reloading through the NetWare system console.
QueuesPerPool	For internal use only; do not modify.
ThreadsPerQueue	For internal use only; do not modify.

Using the NetWare Media Server Option With a Cluster

Server clusters provide high availability and manageability of critical network resources, including data (volumes), applications, server licenses, and services. In a server cluster, two or more servers (called *nodes*) are linked in a network, and run cluster software that allows network resources to be tied to a cluster rather than to individual network servers. With cluster-enabled volumes, your data and applications appear to be provided by a single system, even though the cluster may be composed of several network servers.

When one node fails, the failed node's applications and volumes are transparently restarted on a surviving node (called *failover*) by NetBackup. During failover, most users will not even be aware of the failure.

When the node that failed returns to service, the volumes newly acquired by the failover node migrate to the controlling node (called *failback*).

In a cluster environment, the NetWare Media Server Option is installed on each node in the cluster.

All nodes must be in the same NetWare Directory Services (NDS) tree, must be configured with the IP protocol, and must be on the same IP subnet.

Cluster volumes are mounted on a single physical server. When a node failover occurs, the cluster volume automatically remounts on another node in the cluster.

NetBackup is server volume-centric, meaning that only volumes that are mounted on, or "owned by", a server display. When you create a job, you can only back up volumes that are owned by the NetWare Media Server.

With NetWare 6, you can select a virtual server for the backup, and the cluster volume will always be protected.

If you are running NetWare 5, the NetWare Media Server option offers two ways of protecting volumes on a cluster. In both cases, you create backup jobs through NetBackup for each node in the cluster. In creating these jobs, you can either:

- Create backup jobs for each node in the cluster for only the volumes normally mounted to the node. To automatically protect all volumes during a failover, you then create another backup job for each node that protects all volumes that could mount on the node during failover.
- Create backup jobs for each node in the cluster that protects the entire NetWare File System. With this approach, any volumes mounted on the node at the time the job starts will be backed up.

With the first method, you will get an error if a non-clustered volume is not mounted, and therefore, does not get backed up. A disadvantage with this method, however, is that the backup job containing the clustered volume will always fail except during failover (when the volume is actually mounted on the node).

With creating backup jobs that protect the entire NetWare File System, your jobs will end in success even if the cluster volume is not mounted. The disadvantage with this approach, however, is that you will not be notified if a non-clustered volume is not mounted.

When restoring in a cluster environment, restores are performed in the same way as in a non-clustered environment (see "Performing a Restore" on page 31).

Using Intelligent Disaster Recovery 5

This section details how to use the Intelligent Disaster Recovery (IDR) Option, an option designed to help you quickly and efficiently recover your Novell NetWare servers after a catastrophic disaster.

Using Intelligent Disaster Recovery contains the following topics:

Section	Describes
"About the Intelligent Disaster Recovery Option" on page 44	Key benefits and features of the IDR option.
"Requirements for Using IDR" on page 45	Requirements for installing and using IDR.
"Pre-Disaster Preparation" on page 46	An overview of the IDR preparation steps and how to launch the Intelligent Disaster Recovery Wizard.
"Recovering from a Disaster" on page 49	Procedures for recovering your NetWare servers after a disaster occurs.
"Tips for Maximizing Protection" on page 51	Suggestions for ensuring the maximum protection for your NetWare servers.
"NDS Preparation and Recovery Notes" on page 55	Information on NDS disaster preparation and recovery.
"Command Line Parameters" on page 57	The command line parameters used with IDR.
"Using Other Media Types" on page 63	Which media types can be used to protect your data.
"Frequently Asked Questions" on page 64	Questions frequently asked about IDR, disaster planning, and disaster recovery.

About the Intelligent Disaster Recovery Option

IDR provides a fully automated disaster recovery solution that allows you to quickly and efficiently recover your Novell NetWare servers running the NetWare Media Server Option.

IDR supports NSS volumes, allowing you to quickly get your whole NetWare server up and running again in the event of a disaster.

IDR supports the creation of a CD bootable image file that can be used with a CD burner to create bootable CDs. This disaster recovery solution is intended to recover the NetWare server and requires only the latest full backup media to completely recover a system.

You can also generate floppy disks from the CD bootable image on a local Windows workstation, cutting down on floppy creation time.

If you do not elect to create and use CD bootable images, you can create floppy disks at the server. This disaster preparation effort requires you to down your server, format some floppy disks, install and run the software, and then insert those floppy disks when the on-screen instructions prompts for them.

Choosing the Bootable Media

When creating bootable media through IDR, you can create:

- Floppy disks
- CD-Recordable (CD-R) or CD-Rewritable (CD-RW)

Consider your available hardware and your system BIOS when selecting the type of bootable media you create.

For example, bootable CDs require a BIOS that supports booting from a CD-ROM and third-party CD writing hardware and software to allow burning of ISO 9660 CD images.

Bootable CDs provide faster preparation and recovery than floppy disks; however, floppy disks work on most systems. You can also generate floppy disks on a local workstation from the CD bootable image file NBUDRCD.ISO, which resides in the SYS:\VERITAS\NBU\IDR directory, eliminating the need to down the server for IDR preparation.

Requirements for Using IDR

The following requirements are necessary to protect your servers:

- Your system must be running supported NetWare versions with the latest service packs.

Note Because the versions of NetWare that NetBackup supports change over time, you should always check the Operating System Compatibility List at http://www.support.veritas.com. By selecting the appropriate version of NetBackup and the Compatibility tab, you will be able to select and view this list.

- One current full backup of the NetWare server made with NetBackup for NDMP must be available from which to restore.
- `Format.com` must be available.

Note If using NetWare 5.1, you may need to copy format.com from your license disk.

Additional requirements for using CD-R or CD-RW as the bootable media include:

- A BIOS that supports booting from a CD-ROM.
- Third-party CD writing hardware and software to allow burning of ISO 9660 CD images.

Additional requirements for using floppy disks as the bootable media include:

- Floppy disks must be available during the preparation of this protection scheme.

Note It is strongly recommended that you run chkdsk/scandisk on the floppy disks to verify their integrity.

- The DOS program `Format.com` must reside on the bootable DOS system disk.

You may also want to have:

- One current full backup of the NetWare server's DOS partition made with NetBackup for NDMP using the included Novell TSADOSP.NLM.
- A backup made of the NBUDRCD.ISO file after it is created. (You could also copy this file to a local workstation.)
- An alternative removable media, such as Superfloppy, Jaz, or Zip disk to speed up the preparation and recovery processes if not using bootable CD.

Pre-Disaster Preparation

To successfully recover from a disaster, you must properly prepare for it ahead of time. No matter which bootable media you plan to use, the pre-disaster preparation steps should be performed whenever you:

- Add new support packs.
- Upgrade your system's operating system.
- Modify your hardware configuration.
- Add or modify volumes on your server.

Note If the REMOVE DOS command has been executed from your system console, the Intelligent Disaster Recovery preparation will not work. Down the server and reboot; do not issue the REMOVE DOS command; if the command is found in the AUTOEXEC.NCF file, edit the file and remove the command. Down the server and reboot it.

If NetWare Media Server Option is installed on your server, it must be loaded but not actively running jobs.

Pre-Disaster Preparation for Bootable CD

If you plan to use a CD as your bootable media, you must create the CD bootable image file, and then use third-party software and hardware to place that file on a CD. Your bootable CD and your most recent backups can then allow you to restore your server to its pre-disaster state.

▼ To run IDR preparation for bootable CD:

1. At the system prompt:

   ```
   load nbudr -b -a
   ```

   The preparation process creates the CD bootable image file, NBUDRCD.ISO, in the SYS:\VERITAS\NBU\IDR directory.

Note You must use third party CD writing hardware and software to allow burning of this ISO file on the CD.

You should ensure your computer is capable of booting from the CD (see "Recovering Using a Bootable CD" on page 49).

Pre-Disaster Preparation for Floppy Disks

If you plan to use floppy disks for your bootable media, run pre-disaster preparation steps at the server that include first creating a boot disk and then copying information required to protect your server on floppy disks.

You will need a number of blank, formatted disks if you want to use disks as your bootable media. This number will vary depending on the version of NetWare and other software you have installed in your server.

Number of Disks Required

MINIMUM # OF DISKS REQUIRED FOR THE MEDIA SERVER	MINIMUM # OF DISKS REQUIRED FOR THE REMOTE NETWARE SERVER
NetWare 6.0 or 6.5 - 19 disks	NetWare 6.0 or 6.5 - 17 disks
NetWare 5.1 - 13 disks	NetWare 5.1 - 11 disks

Label the disks as requested by the preparation process.

Note You can substitute alternative media such as Zip, Jaz, or hard disk space (not containing the NetWare partition) in place of floppy disks during the server-based pre-disaster preparation phase. For instructions on using these alternative media types, see "Using Other Media Types" on page 63.

If you elect to generate floppy disks as your bootable media, the first step is to create a boot disk that is used to start the recovery process.

Note It is critical that the boot disk be created properly, and that the server can be successfully booted to DOS when it is used.

▼ **To create the boot disk:**

1. Label the floppy disk *Disaster Recovery System disk*.

2. To format the disk as a system disk, down the server and format the disk using the following command:

   ```
   Format A: /s
   ```

3. Copy the DOS programs FORMAT.COM and FDISK.EXE to the disk.

Note The safest way to create the Disaster Recovery System disk is to follow these steps. By creating the disk at the server, you are ensuring that the correct version of DOS is placed on the disk, and that the appropriate versions of FORMAT.COM and

FDISK.EXE are used. Additionally, not all disk drives are identical although it is more likely that disks created in the drive can be read by that drive; however, we understand that there are servers that you cannot afford to arbitrarily bring down. If this is the case, you can create the Disaster Recovery System disk at another workstation as long as you are using the same versions of DOS, FORMAT.COM, and FDISK.EXE that are on the server you want to protect. *Do not* use Windows 95/98 DOS.

Now that you have a system disk, along with blank disks, it is time to collect the information required to protect your server.

Note If the REMOVE DOS command has been executed from your system console, the Intelligent Disaster Recovery preparation will not work. Down the server and reboot; do not issue the REMOVE DOS command; if the command is found in the AUTOEXEC.NCF file, edit the file and remove the command. Down the server and reboot it.

Note NetWare Media Server Option must be running on the server in order to allow the preparation utility to detect the appropriate NetWare Media Server Option files necessary to recover the server data. If you have not installed NetWare Media Server Option, install it and do a full backup of your server before continuing.

▼ To continue server-based IDR preparation using floppy disks:

1. Start Intelligent Disaster Recovery for NetWare by typing, at the system console prompt:

   ```
   load nbudr -b
   ```

2. Insert each disk as prompted.

3. After all disks are created, the verification process begins automatically. It is important that you verify the disks.

Note If you cannot verify the disks at this time, you should run the command LOAD NBUDR -C as soon as possible. This option allows you to verify the contents of the IDR preparation disks.

In the event of a disaster, the disaster recovery disks and your most current backup media (Full and Differential or Incrementals) are the only items required to perform a complete and automated recovery of your server. For more information about restoring your server using your disaster recovery disks, see "Recovering Using Floppy Disks" on page 50.

Recovering from a Disaster

If your server were to crash right now, you would need the following in order to recover it with Intelligent Disaster Recovery for NetWare:

- The backup of basic DOS, NetWare, and NDS information generated by Intelligent Disaster Recovery for NetWare.
- A full backup of the server's data.
- Any DOS device drivers required to access the media containing the Intelligent Disaster Recovery information, such as Zip device drivers, SCSI drivers, etc. (see "Using Other Media Types" on page 63).

Recovering Using a Bootable CD

Disaster Recovery using a bootable CD requires only the bootable CD and the most recent backups.

▼ To boot a computer using a bootable CD:

1. At the computer being recovered, ensure the bootable CD created by IDR for NetWare is inserted into the CD-ROM.

2. Follow on-screen instructions.

Note If you are testing your bootable media, do not continue when prompted that the Disaster Recovery process will begin. Instead, remove the CD, press <F3>, and reboot the server.

Recovering Using Floppy Disks

If you experience a catastrophic disaster, restore the hardware to a working state and then boot your server using the *Disaster Recovery System Disk*. After the system initializes, follow the on-screen directions. Intelligent Disaster Recovery for NetWare automatically rebuilds both partitions and volumes, and installs a copy of NetWare Media Server Option, which enables you to restore all data from your media.

After reaching this point, restore all of this server's files using NetBackup. For more information, refer to your NetBackup Administrator's Guide.

Note It is important to understand that Intelligent Disaster Recovery for NetWare leaves your NetWare server in a minimal system state. This means that only the files necessary for NetWare to run have been restored. Everything else must be restored from the media containing the Full backup job, or reinstalled manually.

Recovery Notes

- During a recovery, your system must have the same number of hard drives installed as it did during the disaster recovery preparation phase. If you are restoring to a server with a different hard drive configuration, see "Frequently Asked Questions" on page 64.
- If Intelligent Disaster Recovery for NetWare cannot repartition the DOS partition, you can manually repartition and format it using the FDISK.EXE and FORMAT.COM programs found on the Disaster Recovery System disk.

  After rebuilding the DOS partition, run `NBUDRAPP -F` at the DOS prompt from the Disaster Recovery System disk.

Note The - F parameter begins the recovery operation at the point where the DOS files are restored.

- If, after a catastrophic disaster, you rebuild your server with a larger hard drive or drives, Intelligent Disaster Recovery will, during the recovery process, recognize the extra space and prompt you to allocate the extra space to the original non-mirrored NetWare partition. Answer **Yes** to the prompt to increase the NetWare partition size by the amount of extra disk space found by the Intelligent Disaster Recovery procedure.
- If you use a Boot Manager (System Commander, NT, OS/2, etc.), only the current (DOS) configuration will be recovered.

- If you replace a protected drive with one that already contains a DOS partition and the new drive's DOS partition is not the same size as the original, Intelligent Disaster Recovery will want to repartition the new drive to match the original drive's partition size. If you do not want this done, then use FDISK along with FORMAT to manually create the DOS partition size you want.

  After manually creating the DOS partition, start NBUDRAPP using the -F parameter to restore the DOS Disaster Recovery Files disk(s).

Note When manually repartitioning the DOS partition on the new hard drive, make sure there is enough unpartitioned space left on the drive for the NetWare partition.

- If you are using an IBM computer and the drive containing the system's configuration information fails, you must reconfigure the system using the IBM Reference disk prior to running recovery.
- If you are using a Compaq computer and the drive containing the System Configuration Partition fails, Intelligent Disaster Recovery will re-create the partition on the new hard drive; however, you must use the Compaq SmartStart utilities to update the system partition.

Tips for Maximizing Protection

This section offers you tips on gaining additional protection for your NetWare server data by allowing you to modify specific components of Intelligent Disaster Recovery for NetWare. These tips include:

- Modifying certain .INI files to include additional files for protection
- Protecting your server's *entire* DOS partition using Novell's TSADOSP.NLM

It also offers details about Intelligent Disaster Recovery for NetWare's LOG file and the role it plays in the disaster recovery process.

Note To maintain peak server efficiency and to ensure a complete update to the NDS Recovery disk, enter a value of five minutes in the **Delay after command (seconds)** field on the policy's Pre/Post Options dialog box (for example, 300).

After the backup job runs, Intelligent Disaster Recovery for NetWare starts and the NDS Recovery Files disk 1 update begins.

Modifying the .INI Files

Intelligent Disaster Recovery for NetWare uses three .INI files to create a set of recovery disks for your server. These files, installed in the server's SYS:\VERITAS\NBU directory, include:

- *SYSFILES.INI.* Used to create the Disaster Recovery System disk.
- *DOSFILES.INI.* Used to create the DOS Recovery Files disks. It specifies the recovery-critical files to be backed up from the server's *DOS partition*.
- *NETFILES.INI.* Used to create the NetWare Disaster Recovery Files disks. It specifies the recovery-critical files to be backed up from your server's *SYS: volume*.

Each file is a template used by Intelligent Disaster Recovery for NetWare to back up the default file configurations needed to get your server up and running in a minimal state.

You can edit these files to add files and directories you want to protect; however, the SYSFILES.INI and the NETFILES.INI are designed to cover a wide range of environments so it is not necessary to customize them for your server.

If you want to add other files to the protection process, edit the .INI files and add their path and filename designations.

For example, to add all files residing in the C:\SCSI directory on your DOS partition to DOSFILES.INI, edit the file and add the directory location to the existing path and filename designations.

Example Editing the DOSFILES.INI presents you with the following structure. Add the desired path at the end of the DOS file area.

```
[DOS]
FILE=C:\AUTOEXEC.BAT
FILE=C:\CONFIG.SYS
FILE=C:\DOS\EDIT*.*
FILE=C:\DOS\FORMAT.*
FILE=C:\DOS\HIMEM.SYS
FILE=C:\DOS\QBASIC.EXE
FILE=C:\DOS\SYS.*
FILE=C:\SCSI\*.*

[NETWARE]
FILE=%BOOT_DIR%\ETHERTSM.NLM
FILE=%BOOT_DIR%\FDDITSM.NLM
FILE=%BOOT_DIR%\ICMD.NLM
etc...
```

Make sure that as you add filenames, you spell them correctly. Intelligent Disaster Recovery for NetWare will not notify you of an error if it cannot find the specified file.

Certain files, by default, are not backed up, although they are listed in the .INI files.

To include them, edit the file and add the following:

```
Example

FILE=%BOOT_DIR%\PATCHES\NATIVE\*.*
```

Note If you did not install the patches to the %BOOT_DIR%\PATCHES\NATIVE directory, you must change the FILE= line to reflect where the patches were installed.

There are placeholders in DOSFILES.INI designated as %BOOT_DIR%. These placeholders are replaced by the actual boot directory when Intelligent Disaster Recovery for NetWare runs.

Do not edit these placeholders.

Note During installation, Intelligent Disaster Recovery for NetWare places the .INI files in the `SYS:VERITAS\NBU` directory. Review the .INI files to ensure the correct path locations for the specified files. For example, `C:\DOS` is the path DOSFILES.INI looks for when backing up DOS files on your system; however, if you installed DOS files elsewhere, the path location needs to be updated to reflect this.

Using TSADOSP.NLM

Included with Intelligent Disaster Recovery for NetWare is a Novell-supplied TSA named TSADOSP.NLM. Using this TSA allows you to completely backup and restore your server's DOS partition.

After loading this TSA, perform a full backup of your server, including the complete DOS partition. To include the DOS partition in your backup job, select the DOS Server Partition TSA agent, which appears in the backup sources list under the name SERVER_NAME.DOS Server Partition TSA.

Note This TSA switches the processor into *real mode* to access the DOS partition data. This causes a degradation in server performance during the backup operation. Backups of the DOS partition should be reserved for times when the server is not being heavily used.

Because NetBackup must run in *synchronous mode* when using TSADOSP, the Intelligent Disaster Recovery installation program automatically adds the -s (synchronous mode) switch to the NBUSTART.NCF file for you.

This switch should only be removed if you *do not* plan on performing operations with TSADOSP or plan to use post commands to run the disaster recovery preparation of NDS.

The Intelligent Disaster Recovery Log File

The Intelligent Disaster Recovery Log file is found in the SYS:VERITAS\NBU directory. The file, named NBUDR.LOG is an ASCII text file that is created during the initial Intelligent Disaster Recovery for NetWare preparation process. Information is appended to the file as subsequent disaster recovery updates are completed.

Note During the recovery of a server, a NBUDR.LOG file is created in the server boot directory on the DOS partition. This file can be viewed to review the disaster recovery process after the NetWare server has been recovered. The NBUDR.LOG file is also copied to the system control disk and *should* be reviewed to ensure everything you will need during a recovery was gathered.

The log file contains four sections, each detailing information contained on the set of disaster recovery disks created earlier. Refer to the following example:

```
Example

#
MON Mar 10 12:29:28 1997
#

-----------------------------------------------------
SYS:VERITAS\NBU\SYSFILES.INI
-----------------------------------------------------
SYS:VERITAS\NBU\NBUDIAG.FAX
SYS:VERITAS\NBU\NBUDRAPP.EXE
SYS:VERITAS\NBU\NBUDREPP.RES
SYS:VERITAS\NBU\NLMS\NBUDR.NLM
etc...

-----------------------------------------------------
SYS:VERITAS\NBU\DOSFILES.INI
-----------------------------------------------------
C:\AUTOEXEC.BAT
C:\CONFIG.SYS
C:\DOS\HIMEM.SYS
C:\DOS\QBASIC.EXE
C:\NWSERVER\ETHERTSM.NLM
etc...

-----------------------------------------------------
```

```
SYS:VERITAS\NBU\NETFILES.INI
-----------------------------------------------------

SYS:SYSTEM\NBUSTART.NCF
SYS:SYSTEM\NBUSTOP.NCF
SYS:VERITAS\NBU\NBU.BIN
SYS:VERITAS\NBU\ADSMCFG.BIN
etc...

-----------------------------------------------------------
[Server Specific Data --> Single-Server Tree
-----------------------------------------------------------
```

NDS Preparation and Recovery Notes

One of two NDS Tree Types that may reside on your server determines the preparation contents of the NDS Recovery Files disk(s). The two tree types are:

- Multiple-Server Tree (Replication present)
- Single-Server Tree (No replication present)

Multiple-Server Tree (Replication present)

In this environment, only the Server Specific Information contained in the file SERVDATA.NDS is updated, compressed and copied to the NDS Recovery Files disk. The data contained in this file allows for the recreation of the Directory Services Database in the event the hard disk(s) containing the SYS volume fails. Because this is an automatic process, the only intervention on your part will be to log in to the directory. Because the Multiple-Server Tree environment uses replication to update NDS, it is important to understand that once you restore the Server Specific Information from the NDS Recovery Files disk, you should *not* restore Directory Services from media.

Note If your server held a master replica of any partition, use DSREPAIR to designate a new master replica on a different server in the replica ring. Intelligent Disaster Recovery for NetWare prompts you to perform this at the appropriate time during the recovery process (you can also perform this operation prior to performing the recovery). A list of servers in the replica ring is contained in the NBUDIAG.FAX file on the *Disaster Recovery System* disk.

Changing the Replica Type

To change the replica type, run DSREPAIR on another server in the replica ring that has an active read/write replica of the partition. Use the following steps:

1. Load `DSREPAIR`.

   The **Available Options** menu is displayed.

2. Select the **Advanced Options** menu.

3. Select **Replica and Partition Operations**.

4. Choose the partition to edit.

5. Select **Designate this server as the new master replica**.

6. Then, to make sure that time synchronization is set properly, enter the following commands on the server designated to contain the master replica:

```
set default time server type = single
set timesync type = single
set timesync restart flag = on
```

Note If you intend to leave the master replica on this server, enter the following line in the AUTOEXEC.NCF file:

```
set default time server type = single
```

Single-Server Tree (No replication present)

In this environment, the entire Directory Services database is compressed and copied to the NDS Recovery Files disk. Because the entire database is placed on the disk, it is extremely important to keep the information on the disk(s) up-to-date. For example, whenever you add or remove replicas, partitions, volumes, users, and printers.

After this information is restored and the database is opened, NetWare Directory Services is returned to the state it was in at the time of the last NDS Recovery Files disk preparation. You should only have to restore from media those individual objects that had been added since the last preparation. Likewise, you may also have to delete any objects (using the NWAdmin or NetAdmin programs) that were deleted since the last preparation.

Command Line Parameters

The following tables explain the command line parameters that can be used with Intelligent Disaster Recovery for NetWare.

Some switches may be combined. For example, to do a restore of NDS only, while using a zip drive for the IDR media, you would need to use either the **-E** or the **-I** and **-T<drive>** switches with the LOAD NBUDR command.

NBUDR.NLM Server Preparation/Recovery Application Commands

Switch	Operation	Description
-A	Perform disaster recovery image file creation or recover from a bootable CD.	This option creates the bootable image file NBUDRCD.ISO in the SYS:\VERITAS\NBU\IDR directory or performs disaster recovery from a bootable CD.
-A<volume>	Redirect the ISO and data files to another volume.	This option redirects the ISO and data files to another volume. This option may be used if there are free space issues with the SYS volume. **Note** There must be at least 55 MB free space on the SYS volume for the ISO image to be copied from the alternate volume back to the SYS:\VERITAS\NBU\IDR directory. If the ISO file does not reside on the SYS directory, it will not be copied to tapes.
- B	Perform disaster recovery preparation	This performs a Full disaster recovery preparation. For example, `load nbudr -b`.
- C	Perform a verification of prepared disks	This option allows you to verify the contents of the Intelligent Disaster Recovery preparation disks whenever you desire.
- D	Perform DOS Partition disaster recovery preparation only	This backs up only the files listed in the DOSFILES.INI file.

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

Switch	Operation	Description
- E	Perform EMERGENCY NDS Disaster Recovery	Used only with NetWare version 4.1x or greater, this is used only as a last resort if NDS becomes corrupt and used only for single server trees. Using the command `LOAD NBUDR -E`, allows you to manually restore your NDS information from the NDS Disaster Recovery disk.
- F	Restore DOS and NetWare recovery files	This restores DOS and NetWare recovery files.
- I	Force use of Only Server in NDS Tree	This is used only when the software incorrectly determines that the server is in a multi-server tree. This is denoted during NDS file preparation as [Server Specific Data --> Multi-Server Tree].
- L <language>	Language-specific parameter where <Language> = (E)nglish, (F)rançais, (D)eutsch and E(s)pañol	This is used to select the English, French, German, and Spanish languages.
- M	Use monochrome display	This forces the system to use monochrome instead of color.
- N	Perform NDS disaster recovery preparation only	This backs up only the server-specific information required to recover NDS.

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

Switch	Operation	Description
-P<path>	Specify path where FORMAT.COM file resides.	Used during the creation of the bootable image file to specify the path where your FORMAT.COM file resides. If NBUDR finds more than one FORMAT.COM on your system, you will be prompted to choose the correct one to use. This option allows you to specify which FORMAT.COM file to use without being prompted. If you do not have a copy of FORMAT.COM for your server on the boot disk, which would occur if you installed from a Novell bootable CD, you can specify a path on a floppy disk (`LOAD NBUDR -B -A -PA:\`). **Note** Novell's NetWare 5 license disk contains a copy of FORMAT.COM.
- R	Perform Disaster Recovery	This performs the actual recovery of a server, and this parameter is normally issued only from the application. **Note** If you lose a drive that does not contain any portion of the SYS: volume, you can use the -R option to recover just the affected partitions and volumes: Enter **No** when prompted to delete existing partition(s). Next, abort the operation when the first recovery files disk is requested.
- S	Update Storage Environment only	This updates the information on the Disaster Recovery System disk after you add additional drives and volumes to the system.

NBUDR.NLM Server Preparation/Recovery Application Commands (continued)

Switch	Operation	Description
- T<drive>	Allows you to use any DOS-recognized device to recover your Intelligent Disaster Recovery data files (see "Using Other Media Types" on page 63).	Using the – `T<drive>` parameter specifies where all data files normally written to the disaster recovery support disks (DOS Recovery disks, NetWare Recovery Files disks, and the NDS Recovery Files disks) are to be recovered from.
- U	Update Disaster Recovery System disk only	This includes the storage information (partitions and volumes), and the files listed in the SYSFILES.INI file.
- V	A viewing parameter	This enables the viewing of the storage information contained in the Control File (NBUDR.BIN), located on the Disaster Recovery System Disk.
- Z	For use with *bootable* Zip drives and other similar *bootable* devices	– `Z` tells Intelligent Disaster Recovery that Drive A: is a bootable Zip drive or other similar device.

NBUDRAPP.EXE Command Line Parameters

Switch	Operation	Description
-A	Start disaster recovery process from a bootable CD.	This option starts the disaster recovery process using a bootable CD.
- F	Restore DOS and NetWare recovery files	This restores DOS and NetWare recovery files.
- M	Use monochrome display	This forces the system to use monochrome instead of color.

NBUDRAPP.EXE Command Line Parameters (continued)

Switch	Operation	Description
- T<drive>	Allows you to use any DOS-recognized device to recover your Intelligent Disaster Recovery data files (see "Using Other Media Types" on page 63).	Using the – `T<drive>` parameter uses all data files normally written to the disaster recovery support disks (DOS Recovery disks, NetWare Recovery Files disks, and the NDS Recovery Files disks) on the DOS-recognized drive specified as part of the parameter.
- Z	For use with *bootable* Zip drives and other similar *bootable* devices	– `Z` tells Intelligent Disaster Recovery that Drive A: is a bootable Zip drive or other similar device.

The following table explains the commands that can be used with the disk creation utility, MKIDRDSK.EXE.

MKIDRDSK Command Switches

Switch	Operation	Description
/D	Generate only the DOS images , or when used in with the /F command, generate only the DOS images and disks.	This command creates images of the DOS floppy disks needed for disaster recovery from the image file, and places these images on the media server.
/F	Generate floppy disks.	This command creates and verifies all floppy disk images from the bootable image required to run disaster recovery.
/FO	Create floppy disks from the existing floppy disk images.	This command creates floppy disks from the current floppy disk images without generating the floppy images again.
/H	Display this help screen.	This command displays the help file.

MKIDRDSK Command Switches (continued)

Switch	Operation	Description
/L <language>	Language-specific parameter where <Language> = (E)nglish, (F)rançais, (D)eutsch and E(s)pañol	This is used to select the English, French, German, and Spanish languages.
/N	Generate only images of NetWare floppy disks. If used with the /F command, generate images and floppy disks of the NetWare floppy disks only.	This command creates images of the NetWare floppy disks needed for disaster recovery from the image file, and places these images on the media server.
/S	Generate only an image of the *Disaster Recovery System* disk. If used with the /F command, generate image and floppy disk of the *Disaster Recovery System* disk only.	This command creates an image of the Disaster Recovery System disk from the image file, and places this image on the media server.
/T	Generate only images of NDS floppy disks. If used with the /F command, generate images and floppy disks of the NDS floppy disks only.	This command creates an image of the NDS floppy disks, and places this image on the media server.
/ V	Verify disk images.	This command verifies the disk images.
/Z	Turn on debug.	This command places the MKIDRDSK utility in debug mode.
/ZL	Turn on debug with logging.	This command places the MKIDRDSK utility in debug mode and create a log file.

Using Other Media Types

This section discusses the most common Disaster Recovery preparation procedures using media other than disks. Instead of using disks to create the Intelligent Disaster Recovery disks, you can use the following media types if you have them installed on your system:

- Iomega Zip drives
- Iomega Jaz drives
- Hard disk drives that contain a DOS partition but do not contain a NetWare partition

Using these devices speeds up Intelligent Disaster Recovery for NetWare's disaster recovery preparation and collection process.

Using Zip, Jaz, or Hard Disk Space

Rather than using a set of floppy disks during pre-disaster preparation and server information collection phase, you can use Zip or Jaz cartridges, or hard disk space; however these devices must be seen under DOS, and be assigned a DOS drive letter.

You will still need to create a Disaster Recovery System disk. After creating this system disk, make sure ALL drivers required for the Zip, Jaz, or hard disk drives are copied to the system disk.

1. Create a bootable Disaster Recovery System disk by downing the server and formatting a floppy disk with the following command:

   ```
   FORMAT A: /S
   ```

2. Copy FORMAT.COM and FDISK.EXE to the system disk.

3. Copy all required Zip, Jaz or hard disk drivers to the bootable system disk.

4. Reboot the server with the Disaster Recovery System disk, making sure all devices appear under DOS when the boot procedure finishes.

5. Down the server and reboot it to NetWare.

6. At the System Console, type:

   ```
   load NBUDR -B -T<Alternative media drive letter>
   ```

   For example,

   ```
   load NBUDR -B -TE
   ```

   where E is the drive letter assigned to a Zip drive under DOS.

Intelligent Disaster Recovery now collects all pertinent server recovery data and places it on the alternative media specified with the **-T** switch, instead of on floppy disks.

Frequently Asked Questions

I used to have three 1GB hard drives on my server when it crashed. I've replaced them with a single 3GB hard drive. How do I use Intelligent Disaster Recovery to restore my system?

You will need to boot from the *Disaster Recovery System disk* and once loaded, press <F3> to exit to DOS. Run FDISK.EXE from the floppy and recreate the DOS Partition(s) manually.

Note If you don't remember the size of the DOS Partition(s) you can run NBUDRAPP -Z to display the partition information.

After the system reboots and NBUDRAPP is reloaded, press <F3> to exit to DOS. Run FORMAT.COM from the floppy to format the DOS Partition(s).

Next run NBUDRAPP -F to recover the DOS Data Files from the DOS Recovery Files disk(s) and allow the recovery process to continue to bring up NetWare. After the server is restarted and NBUDR.NLM is loaded, you are informed that *There are too few Hard Disks! Original* = #, *Current* = #. Press a key to exit the application. From the system console, load INSTALL and manually recreate the NetWare Partition(s) and Volume(s)

Note Don't forget to add the Name Spaces back to the Volume(s). If you don't remember the size of the NetWare Partition(s) or Volume(s), load NBUDR -V to display the partition information and volume information.

Next, load NBUDR -F to recover the NetWare Data Files. Load NBUDR -E to recover Directory Services. Once this is complete you can execute NBUSTART.NCF to start the NetWare Media Server Option. After it loads, catalog and restore the media required to get back your data.

I used to have an IDE hard drive in my server and now I am upgrading to a SCSI drive that is a bit bigger. How do I use Intelligent Disaster Recovery to restore my server?

Make sure the BIOS is enabled for the SCSI card (so DOS will recognize the drive without the need for additional drivers) and just perform a normal recovery. During the NetWare Partition recovery process, a prompt states that additional space is available for NetWare and gives you the option of using it.

Note If you don't use it you will NOT be able to allocate it to NetWare later.

The recovery process proceeds normally from this point.

The hard disk controller in my system has changed. How do I use Intelligent Disaster Recovery to restore my system?

Before performing the Intelligent Disaster Recover Preparation, add the additional SCSI drivers (for the new controller) to the DOSFILES.INI file in the [NetWare] section.

If you haven't done this and are using floppy disks for the recovery, reboot from the system floppy disk, and then press <F3> to exit to DOS.

Next, copy the required drivers to the server boot directory (nwserver) and edit the STARTUP.NCF file and add the new drivers.

Manually copy the AUTOEXEC.NCF from the floppy to the server boot directory and execute SERVER.EXE.

Recovery should continue normally from this point.

The server I am restoring is not the media server. How do I use Intelligent Disaster Recovery to restore my system?

There is no difference between installing Intelligent Disaster Recovery remotely on a remote server or locally on a media server. Make sure, however, you have a full backup of the remote server on the media server's tape drive. After the remote server backup is done, perform the Intelligent Disaster Recovery installation and preparation process on the actual remote server.

If a disaster does occur, simply perform Intelligent Disaster Recovery for NetWare's recovery process on the remote server. After the disaster recovery process completes, restore the server's data from your backup tapes.

Why do I need to have NetWare Media Server Option loaded in order to prepare the disaster recovery floppy disks?

This only occurs when you are doing a Disaster Recovery Preparation on a server that has NetWare Media Server Option installed. The Disaster Recovery process restores a minimal NetWare Media Server Option installation as well as getting your NetWare system to a running state. The preparation process needs NetWare Media Server Option loaded in order to determine which NLMs should be saved on the Disaster Recovery disks.

Just the drive that has the SYS: volume failed on my server. How do I use Intelligent Disaster Recovery to restore my system?

Run the Intelligent Disaster Recovery normally. When prompted to delete existing partitions (this happens once NBUDR.NLM is loaded and determines NetWare partitions already exist) say "No." Recovery will proceed normally.

The tape drive that I am using to restore my system is not the same as the one that was being used when the Disaster Recovery Preparation was done for the media server. How do I restore my system?

If the tape drive requires a media type different than what was used to do the original backup of the server, you will not be able to perform a restore.

However, if the same media can be used but the tape drives are housed in a different manner (stand-alone versus autoloader), then the NetWare Media Server Option must be re-installed before restoring the data. If you do not re-install the software, the recovery will still work, but you will get an error stating that no tape drives are found when the NetWare Media Server Option is launched.

For example, if you've replaced a stand-alone 4mm DAT tape drive with a 4mm autoloader device, you will need to re-install the NetWare Media Server Option on your server before restoring the data.

Index